WLAN IP Telephony Installation and Configuration Guide

BCM

Business Communications Manager

Document Status: **Standard**

Document Number: **NN40010-303**

Document Version: **01.01**

Date: **January 2008**

NORTEL

Copyright © 2005–2008 Nortel Networks, All Rights Reserved

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Trademarks

Nortel, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

Microsoft, MS, MS-DOS, Windows, and Windows NT are trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Task list

To wall-mount the WLAN IP Telephony Manager 2245 49
To rack-mount the WLAN IP Telephony Manager 2245....50
To connect the power 50
To configure the WLAN IP Telephony Manager 2245 52

To connect to the WLAN IP Telephony Manager 2245 through a serial port 53
To connect to the WLAN IP Telephony Manager 2245 through Telnet....54
To save the configuration 58
To change the password 61
To open and use the Admin menu on the wireless handset....64
To make an alphanumeric string entry 65
To download the wireless handset software....79
To program the keys on the wireless handset....85
To install and configure the configuration cradle 86
To read and save the configuration of an existing handset 92
To create a new master configuration file....93
To create a new configuration using the master files 93
To change an existing configuration file 93
To change a configuration obtained from a handset 94
To download a configuration to a handset....94
To test the wireless handsets 95
To test signal strength using the wireless handset....103
To initiate a PTT call....106
To replace a WLAN IP Telephony Manager 2245....110
To view the software version 111
To install the WLAN Application Gateway 2246 145
To connect to the WLAN Application Gateway 2246 through a serial port....146
To configure the system type from the OAI Box Configuration option....149
To configure the network 150
To connect the WLAN Application Gateway 2246 to the LAN....152
To connect to a WLAN Application Gateway 2246 through Telnet 154
To configure a telephone line 156
To delete a handset....157
To search for a handset....157
To program a feature....158
To set or change a password 159
To certify wireless handsets on an existing system....164
Transferring the software using FTP 165
To load software updates 166
To use the serial port as the Application Server communication link 168

Contents

Task list 3

Contents 5

Chapter 1
Getting started 11

About this guide 11
Audience 11
Acronyms 11
Symbols and text conventions 13
Related publications 14
How to get Help 15
Getting Help from the Nortel Web site 15
Getting Help over the phone from a Nortel Solutions Center 15
Getting Help through a Nortel distributor or reseller 15

Chapter 2
Overview 17

Wireless telephone network description 17
Call Server 17
DHCP Server 17
Firewall 17
WLAN Handset 2210, WLAN Handset 2211, and WLAN Handset 2212 18
Language 18
Licenses 18
Wi-Fi Multimedia (WMM) 19
Wired Equivalent Privacy (WEP) 19
Wi-Fi Protected Access (WPA) 19
Wi-Fi Protected Access2 (WPA2) 19
Virtual Private Network (VPN) 19
Push-to-talk feature 19
Loud noise environments 20
WLAN IP Telephony Manager 2245 20
WLAN Application Gateway 2246 20
Access Points 21
Handset switchover 21
Loss of signal 21

Chapter 3
Planning 23

DHCP server planning 23
TFTP Server planning 24
Syslog Server planning 25
AP planning 25
Site survey 25
Conducting an effective site survey 28
Example of AP placement 29
Solving coverage issues 31
Solving overlap issues 31
Network planning 31
Zones 31
WLAN IP Telephony Manager 2245 planning 32
Installation requirements 32
WLAN IP Telephony Manager 2245 groups 32
2245 Model 10 and Model 20 server capacities 34
Gateway and timing function 34
Multicast 35
WLAN Application Gateway 2246 planning 36
Installation requirements for the WLAN IP Telephony Manager 2245 and the WLAN Application Gateway 2246 36
IP address planning 36
IP addressing with DHCP 37
Planning worksheets 37

Chapter 4
System information 41

Bandwidth management 41
Zones 41
Zones for wireless handsets 41
Call blocking 42
Codecs 43
RLR and SLR 43
RTCP 43
Gain adjustment 44
Programmable rings and tones 44
In/Out of Service tones 44
Local mode display 44
Survivable Remote Gateway 45
External Applications Server 45
End-to-end QoS 45

NAT 46
IP Phone 2004 features 46

Chapter 5
Installation 47

Required materials 47
Supplied equipment 47
Pre-installation checklist 47
Installing the WLAN IP Telephony Manager 2245 48
About the front panel 48
Wall mounting 49
Rack-mounting 49
Connecting to the LAN 50
Connecting to the power 50
Installing the WLAN Application Gateway 2246 50

Chapter 6
WLAN IP Telephony Manager 2245 configuration 51

Functional description 51
Configuration tasks 52
Connecting to the WLAN IP Telephony Manager 2245 53
Through a serial port 53
Through Telnet 54
Configuring the network 55
Saving the configuration 58
Changing the master IP address 58
Configuring the WLAN IP Telephony Manager 2245 58
Changing the password 61

Chapter 7
WLAN Handset configuration 63

System provisioning 63
Configuring the handset 63
Configuring the handset using the configuration cradle 63
Opening and using the Admin menu on the handset 64
Admin menu options 65
License Option 69
Terminal Type 69
OAI On/Off 69
Push-to-talk 70
Admin Password 70
IP Addresses menu 70
ESSID 72

Security 73
Reg. (Regulatory) Domain 77
Transmit Power 77
Run Site Survey 77
Diagnostics Mode 78
Syslog Mode 78
Restore Defaults 78
Downloading the wireless handset software 79
Pre-download checklist 79
Downloading the software 79
IP Phone 2004 mapping 80
Voice Messaging Access 80
Codecs 80
DHCP 80
TFTP 81
DNS 81
Feature programming 82
Feature and key assignment 82
Program keys on the wireless handset 85
Configuration cradle 85
Using the configuration cradle and software 88
Planning the configuration files 89
Configuration cradle software 90
Reading and saving a handset configuration 91
Testing the wireless handsets 94
Diagnostic Tools 95
Run Site Survey 95
Diagnostics Mode 96
Syslog Mode 100
Site certification 103
Testing signal strength with the handset 103
Push-to-talk 105
PTT operation 106
User-defined preferences 107
Configuration cradle worksheet 108

Chapter 8
Administration and maintenance 109

Adding a WLAN IP Telephony Manager 2245 to the system 109
Checking in to the Gateway 109
Replacing a WLAN IP Telephony Manager 2245 109
Failed master WLAN IP Telephony Manager 2245 109

Replacing the failed WLAN IP Telephony Manager 2245 109
Removing a WLAN IP Telephony Manager 2245 from the system 110
Wireless handset scenarios 110
Changing the master WLAN IP Telephony Manager 2245 111
Viewing software version 111
For the WLAN IP Telephony Manager 2245 111
For the WLAN Application Gateway 2246 113
For a wireless handset 113
Updating software 113
Updating software on the WLAN IP Telephony Manager 2245 113
Updating software on the WLAN Application Gateway 2246 114
Updating software on a wireless handset 114
Displays 115
Wireless handset download messages 115
Normal download messages 115
Download failure or recovery messages 116

Chapter 9
Troubleshooting 117

Troubleshooting the WLAN IP Telephony Manager 2245 117
Error Status screen 118
Network Status screen 118
Software Version Numbers screen 120
Speed or duplex mismatch 121
Troubleshooting the WLAN Application Gateway 2246 121
Troubleshooting the handset 121
Context 121
Access Point problems 121
Configuration problems 122
Duplex mismatch 122
No ring 122
Far-end echo 123
Dropped calls 123
Wireless handset status messages 123
Using Call Server overlay commands 134
LD 32 IDU command 134
LD 32 STAT command 135
LD 117 Inventory command 136
LD 117 STIP command 136
TPS CLI commands 136
Determining alias IP addresses 139
Troubleshooting coverage issues 139

Before calling Nortel Technical Support 139
WLAN Application Gateway 2246 141
System overview 142
Front panel 143
Third-party applications 144
Nurse-call systems 145
Installation 145
Installing with a new system 145
Installing in an existing system 145
Configuring the WLAN Application Gateway 2246 IP address 146
Configuration 147
Navigating the Administration console 147
Task summary list 149
Connecting to the Application Server 152
Continuing configuration through Telnet 154
Connecting through Telnet 154
Configuring the Telephone Line 155
Deleting a handset 157
Searching for a handset 157
Programming a feature 158
Setting or changing a password 159
Viewing system status 159
Viewing network status 160
Viewing Telephone Line Status 162
Viewing software versions 163
WLAN Application Gateway 2246 certification 163
Wireless handset certification 163
Updating software 164
Software updates 164
TFTP software updates Systems 166
Planning Worksheet for Handsets 167
Freeing the serial port for administrative purposes 168
Compatible Access Points 169

Index 171

Chapter 1
Getting started

This document is a global document. Contact your system supplier or your Nortel representative to verify that the hardware and software described are supported in your area.

This section contains information on the following topics:

- "About this guide" on page 11
- "Related publications" on page 14
- "How to get Help" on page 15

About this guide

This document describes the planning, installation, configuration, maintenance, and troubleshooting for the Nortel WLAN system, including the following elements:

- Nortel WLAN IP Telephony Manager 2245
- Nortel WLAN Application Gateway 2246 (optional)
- Nortel WLAN Handset 2210
- Nortel WLAN Handset 2211
- Nortel WLAN Handset 2212

Audience

This guide is intended for planners and installers of WLAN systems, as well as for individuals responsible for configuring, maintaining, and troubleshooting the WLAN system.

Acronyms

The following is a list of acronyms used in this guide.

Table 1

Acronym	Description
AP	Access point
AES	Advanced Encryption Standard
BB	Best bandwidth
BCM	Business Communications Manager
BQ	Best quality
CFNA	Call Forward No Answer

Table 1

Acronym	Description
CRC	Cyclic redundancy check
DHCP	Dynamic Host Configuration Protocol
DNS	Domain name services
DS	Direct sequence
DSSS	Direct sequence spread spectrum
ESSID	Extended service set identifier
FH	Frequency hopping
FSR	Fast secure roaming
LAN	Local area network
LTPS	Line telephone proxy server
NAT	Network address translation
OAI	Open application interface
PSK	Pre-shared key
PTT	Push-to-Talk
QoS	Quality of Service
RLR	Radio frequency
RLR	Receive loudness rating
RTCP	Real-time Transport Control Protocol
SLR	Send loudness rating
SNMP	Simple Network Management Protocol
SRG	Survivable Remote Gateway
SSC	Small system controller
SVP	SpectraLink voice prioritization
TFTP	Trivial File Transfer Protocol
VPN	Virtual private network
WEP	Wired equivalent privacy
WLAN	Wireless local area network
WMM	Wi-Fi multimedia
WNS	Window name services
WPA2	Wi-Fi protected access2
WPA	Wi-Fi protected access
WSS	Wireless security switch

Symbols and text conventions

These symbols are used to highlight critical information for the BCM system:

Caution: Alerts you to conditions where you can damage the equipment.

Danger: Alerts you to conditions where you can get an electrical shock.

Warning: Alerts you to conditions where you can cause the system to fail or work improperly.

Note: A Note alerts you to important information.

Tip: Alerts you to additional information that can help you perform a task.

Security note: Indicates a point of system security where a default should be changed, or where the administrator needs to make a decision about the level of security required for the system.

Warning: Alerts you to ground yourself with an antistatic grounding strap before performing the maintenance procedure.

Warning: Alerts you to remove the BCM main unit and expansion unit power cords from the ac outlet before performing any maintenance procedure.

These conventions and symbols are used to represent the Business Series Terminal display and dialpad.

Convention	Example	Used for
Word in a special font (shown in the top line of the display)	Pswd:	Command line prompts on display telephones.
Underlined word in capital letters (shown in the bottom line of a two line display telephone)	PLAY	Display option. Available on two line display telephones. Press the button directly below the option on the display to proceed.
	#	you press on the to select a particular option.

These text conventions are used in this guide to indicate the information described:

Convention	Description
bold Courier text	Indicates command names and options and text that you need to enter. Example: Use the **info** command. Example: Enter **show ip** {**alerts**|**routes**}.
italic text	Indicates book titles
plain Courier text	Indicates command syntax and system output (for example, prompts and system messages). Example: Set Trap Monitor Filters
FEATURE HOLD RELEASE	Indicates that you press the button with the coordinating icon on whichever set you are using.
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.

Related publications

Related publications are listed below.

WLAN Handset 2210/2211/2212 User Guide (NN40050-101)

IP Line: Description, Installation, and Operation (553-3001-365)

How to get Help

This section explains how to get help for Nortel products and services.

Getting Help from the Nortel Web site

The best source of support for Nortel products is the Nortel Support Web site:

http://www.nortel.com/support

This site enables customers to:

- download software and related tools
- download technical documents, release notes, and product bulletins
- sign up for automatic notification of new software and documentation
- search the Support Web site and Nortel Knowledge Base
- open and manage technical support cases

Getting Help over the phone from a Nortel Solutions Center

If you have a Nortel support contract and cannot find the information you require on the Nortel Support Web site, you can get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7865).

Outside North America, go to the Web site below and look up the phone number that applies in your region:

http://www.nortel.com/callus

When you speak to the phone agent, you can reference an Express Routing Code (ERC) to more quickly route your call to the appropriate support specialist. To locate the ERC for your product or service, go to:

http://www.nortel.com/erc

Getting Help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, you can contact the technical support staff for that distributor or reseller.

Chapter 2
Overview

Wireless telephone network description

The Nortel WLAN wireless telephone network consists of the following components:

- Call Server
- DHCP server
- Trivial File Transfer Protocol (TFTP) server
- Firewall
- Nortel WLAN Handset 2210, Nortel WLAN Handset 2211 and Nortel WLAN Handset 2212
- Nortel WLAN IP Telephony Manager 2245
- Nortel WLAN Application Gateway 2246 (optional)
- Access Point (AP) — one or more as required by the site

Call Server

The Call Server can be the Call Server of a Business Communications Manager (BCM) system running BCM software.

DHCP Server

The existing DHCP Server can be on either side of the firewall, according to the site administrator's preference. The DHCP server is optional if the wireless handsets and WLAN IP Telephony Manager 2245 are statically configured.

TFTP Server

A TFTP Server is required in an IP Telephony system to distribute software to the wireless handsets and WLAN IP Telephony Manager 2245. It can reside on a different subnet than the Call Server and APs. The TFTP Server can be located on either side of the firewall.

Firewall

The firewall is an optional element that is often used to separate the wireless and wired domains.

WLAN Handset 2210, WLAN Handset 2211, and WLAN Handset 2212

The WLAN Handset 2210, WLAN Handset 2211 and WLAN Handset 2212 use Voice over IP (VoIP) technology on IEEE 802.11-compliant Wireless Local Area Networks (WLAN). APs use radio frequencies to transmit signals to and from the wireless handsets.

Note: In this document, handsets means the WLAN Handset 2210, WLAN Handset 2211, and WLAN Handset 2212. Where the feature refers only to a specific handset, the full handset name is used.

Employees carry wireless handsets to make and receive calls as they move throughout the building. The handsets are used only on the premises; they are not cellular phones. The handsets communicate with the BCM system and with the WLAN IP Telephony Manager 2245. Just like wired telephones, the wireless handsets receive calls directly, receive transferred calls, transfer calls to other extensions, and make outside and long-distance calls (subject to corporate restrictions).

The handsets interoperate with other IP Line and IP Trunk features and devices, such as IP Peer, and the IP Phone 20xx and IP Softphone 2050 series of IP Phones, with the exception of some media-related constraints described in "Codecs" on page 43.

The radio frequencies use spread spectrum radio technology, that comes in two variations:

- direct sequence (DS)
- frequency hopping (FH)

The handsets use DS spread spectrum radio technology to optimize bandwidth and minimize jitter on the WLAN. The wireless handsets are not compatible with FH.

The handsets on an 802.11a/b/g network operate at a transmission rate of up to 11 Mb/s in a direct sequence spread spectrum (DSSS) system.

Language

The handset menus and screens that originate from the Call Server are displayed in the languages supported on the Call Server. The administration and configuration menus, and all other local handset prompts are English-only.

Licenses

The handset appears to the Call Server as a standard IP Phone 2004. Therefore, each wireless handset requires one IP User License and is subject to the same feature packaging requirements as the existing IP Phone 2004.

Wi-Fi Multimedia (WMM)

The handsets support basic Wi-Fi Multimedia (WMM) to improve Quality of Service (QoS), as defined in the 802.11e specification. WMM provides prioritized QoS capability when concurrent applications, each with unique latency requirements, are competing for network resources.

When WMM is used, all voice traffic originating from the wireless handset is assigned the WMM Voice Access Category, making it the highest priority application. If the wireless network supports WMM, the handsets enable WMM support automatically; otherwise, SpectraLink voice prioritization (SVP) is used.

Wired Equivalent Privacy (WEP)

The handsets support Wired Equivalent Privacy (WEP) as defined by the 802.11a/b/g specification. Nortel offers the product with both 40-bit and 128-bit encryption. WEP increases the security of the wireless LAN to a level similar to a wired Ethernet LAN.

Wi-Fi Protected Access (WPA)

The handsets support Wi-Fi Protected Access (WPA) using Pre-Shared Key (PSK), as defined by the 802.11i specification. WPA increases the security of the wireless LAN, using key encryption, key rotation, authentication and message integrity checking.

Wi-Fi Protected Access2 (WPA2)

The handsets support Wi-Fi Protected Access2 (WPA2) using PSK and Advanced Encryption Standard (AES), as defined by the 802.11i specification. WPA2 increases the security of the wireless LAN, using key encryption, key rotation, data encryption, authentication and message integrity checking.

Virtual Private Network (VPN)

The WLAN Handset 2212 supports Virtual Private Network (VPN) security. VPN security provides a secure tunnel for the transfer of unencrypted information. A two-phase approach is used to negotiate the tunnel, with Phase 1 protecting Phase 2. Phase 1 uses pre-shared keys, Diffie-Hellman group, hashing, and encryption. Phase 2 uses hashing and encryption. Both phases have limited, configurable lifetimes.

Push-to-talk feature

The Push-to-talk (PTT) feature allows the WLAN Handset 2211 to operate in a PTT group-broadcast mode like a two-way radio, in addition to the standard telephone operation.

For more information, see “Push-to-talk” on page 105.

Loud noise environments

The handsets are designed to provide optimal voice quality. However, when used in extremely loud noise environments, (for example, close to working heavy machinery), degradation in call quality may be experienced due to echo. Avoid using the handsets in loud noise environments

WLAN IP Telephony Manager 2245

The WLAN IP Telephony Manager 2245 is a device that manages IP telephony network traffic on the WLAN system. It is required to utilize the 11 Mb/s maximum transmission speed available in the handsets. The WLAN IP Telephony Manager 2245 acts as a proxy for the wireless handsets. It provides a number of services including a QoS mechanism, AP bandwidth management, and efficient RF link utilization.

The WLAN IP Telephony Manager 2245 works with the APs to provide QoS on the WLAN. All voice packets are encapsulated by the wireless handsets. The encapsulated voice packets to and from the wireless handsets are handled by the WLAN IP Telephony Manager 2245 and routed to and from a Call Server.

SpectraLink Voice Priority is the QoS mechanism implemented on the wireless handsets and APs to enhance voice quality over the wireless network. SVP gives preference to voice packets over data packets on the wireless medium, increasing the probability that all voice packets are transmitted and with minimum delay. SVP is fully compliant with the IEEE 802.11 and 802.11a/b/g standards.

Each subnet where the wireless handsets will operate requires at least one WLAN IP Telephony Manager 2245. One unit can process 80 simultaneous calls. If greater capacity is required, multiple units can be used in a master-slave arrangement.

Table 1 WLAN IP Telephony Manager 2245 model and capacities

Model	Capacities
2245	80 simultaneous users
2245 Model 10	10 total users
2245 Model 20	20 total users

WLAN Application Gateway 2246

The WLAN Application Gateway 2246 is an optional device that enables third-party applications to communicate directly with up to 10,000 wireless handsets. The WLAN Application Gateway 2246 is connected to the LAN Ethernet switch through an RJ-45/CAT5 cable.

For more information on the WLAN Application Gateway 2246, see Appendix A, “WLAN Application Gateway 2246.

A WLAN Application Gateway 2246 supports 64 to 10,000 wireless handsets, depending on the model of Gateway, as listed in Table 2.

Table 2 WLAN Application Gateway 2246 models and capacities

Model number	Maximum number of users
NTTQ65AA	64
NTTQ65BA	128
NTTQ65CA	256
NTTQ65DA	512
NTTQ65EA	1024
NTTQ65FA	10000

Access Points

802.11a/b/g APs provide the connection between the wired Ethernet LAN and the wireless (802.11) LAN. APs must be positioned in all areas where the wireless handsets will be used. The number and placement of APs affects the coverage area and capacity of the wireless system. Typically, the requirements for use of handsets are similar to that of other wireless data devices.

The APs must be either SVP-compliant or WMM-compliant to support QoS. For a list of supported APs, see Appendix B, “Compatible Access Points.

Handset switchover

When a user on an active call is moving about, the call switches from AP to AP in the subnet. This changeover is transparent to the user.

Loss of signal

If a wireless handset is out of range of all APs, it waits 20 seconds for a signal to return. If a signal is not re-acquired within 20 seconds, the wireless handset loses connection to the Call Server and any calls are dropped. When the wireless handset comes back into range of an AP, it re-establishes a connection to the Call Server and goes through the system registration process.

If a wireless handset is out of contact with the system for four seconds (worst case scenario) when the UNIStim messaging is occurring, then a UNIStim failure could result, causing the wireless handset to lose the UNIStim association with the Line Telephony Proxy Server (LTPS).

Chapter 3
Planning

DHCP server planning

The handset IP-related parameters can be configured manually or through a DHCP server (RFC 1541 and RFC 1533). Any DHCP server can be used, but it must support the following capabilities.

Note: There is no partial DHCP mode, as there is with an IP Phone 2004. Therefore, the DHCP server must support the options marked with a "*".

- * Provide Client IP address
- * DHCP Option 1 – Subnet Mask
- * DHCP Option 3 – Default Gateway
- * DHCP Option 60 – Class Identifier. The wireless handsets use the Class Identifier of "Nortel- 221x-A". The DHCP server can use the string in the Class Identifier to uniquely identify a wireless handset.
- * DHCP Option 66. This can be used to specify the address of the TFTP Server. If this option is not configured, the wireless handset looks at the Next server/ Boot server (siaddr) Option for the address of the TFTP Server* Vendor Specific Option 43, 128, 144, 157, 191, or 251. Only one of these options is required. The DHCP server encodes the Server 1 information using the same format as the IP Phone 2004. If the Server 2 information is also present in the option, it is ignored.
- * DHCP Option 151. This option contains the IP address of the WLAN IP Telephony Manager 2245. If Option 151 is not configured, the wireless handset performs a DNS lookup of the name "SLNKSVP2", if Options 6 (DNS Server) and 15 (Domain Name) are configured.
- DHCP Option 152. If an optional WLAN Application Gateway 2246 is used in the system, its IP address can be specified with this option.

Each wireless handset effectively uses two IP addresses in the wireless subnet: one for the physical wireless handset and a second alias IP address that is used on the WLAN IP Telephony Manager 2245. When allocating addresses in a subnet scope on the DHCP server, a contiguous block of IP addresses as large as the number of wireless handsets supported must be marked as unavailable for distribution for other uses by the DHCP server.

When multiple WLANs are connected to a single Nortel wireless security switch (WSS), the DHCP server can require specific configuration modifications. Please refer to the documentation for the specific WSS being used for any special DHCP configuration requirements.

TFTP Server planning

A TFTP Server (RFC1350) holds the software images for updating the handsets and the WLAN IP Telephony Manager 2245. When the IP address of the TFTP server has been configured on the wireless handset, each time a wireless handset is powered on, the wireless handset checks its version of firmware against the firmware on the TFTP Server, and if the version is different, the wireless handset downloads the new firmware from the TFTP Server. Similarly, when a WLAN IP Telephony Manager 2245 reboots, or is manually reset by the operator, it checks its version of software against the version on the TFTP Server. If the versions are different, the WLAN IP Telephony Manager 2245 downloads the new software.

The following information must be considered when planning for a TFTP Server:

- The process for the wireless handset to check its version of firmware against what is available on the TFTP Server takes less than two seconds on a quiet network.
- If the TFTP Server is offline or unreachable, the wireless handset tries for about 10 seconds before giving up and using its existing version of firmware.
- The wireless handset firmware downloading process takes about 30 seconds.
- The TFTP Server must be capable of supporting multiple TFTP sessions.
- When a wireless handset makes a TFTP request, it uses file names without a full path name. Therefore, software updates for the WLAN IP Telephony Manager 2245 and handsets must be installed into the root directory of the TFTP Server.

When the software files are uploaded to the TFTP server. they must be unzipped. Allow time for the TFTP server to refresh and be aware of the files before attempting to download software to the wireless handsets and WLAN IP Telephony Manager 2245. Monitor the TFTP Server for any errors.

The TFTP Server can be located anywhere on the network if the wireless handsets have the subnet mask and default IP gateway configured correctly. However, the wireless handset expects a response within two seconds to any TFTP request. Therefore, the TFTP Server should not be located, for example, at the other end of a slow WAN link.

If too many wireless handsets are attempting to download new software simultaneously, the downloads can slow down or return error messages. To reduce the number of retries and error messages, manage the download process by staggering the times the wireless handsets download the software.

Nortel has tested the following TFTP servers. They are listed in order of preference.

- Nortel TFTP server (ONMS application)
- 3COM TFTP
- PumpkinTFTP

Syslog Server planning

A Syslog Server listens for incoming syslog messages on UDP port 514 and then processes the messages according to local administrative procedures. Usually the syslog messages are logged for subsequent review by the system operator. A number of devices used within a handset wireless configuration are capable of sending messages to a Syslog Server.

The Syslog Server can be any RFC 3164-compliant log server. The WLAN IP Telephony Manager 2245, Wireless Security Switches 2250/2270, WLAN Application Gateway 2246, and WLAN APs 2220/2221/2230/2231 can be configured to generate syslog messages. Refer to the documentation for the Wireless Security Switches and WLAN APs for information on configuring syslog messages. For information on configuring syslog messages on the WLAN IP Telephony Manager 2245, see "Configuring the network" on page 55.

There are numerous third-party Syslog Servers available. Any RFC 3164-compliant Syslog Server can be used.

AP planning

APs utilize radio frequencies to transmit signals to and from the wireless handsets.

It is essential to know where to install the APs to provide effective coverage for wireless handset use. It is necessary to verify that coverage is available where it is needed. The first step is to define exactly where the coverage is needed, which requires a site survey.

Recommendation

A site survey must be performed before installing a wireless LAN. A site survey is also recommended when an existing network structure is modified or when physical changes are made to a site.

Nortel recommends the use of the Nortel Site Survey Tool to perform the site survey.

A site survey is critical to designing and implementing a wireless LAN. The site survey is used to determine the number of APs needed to support the wireless handset users and to determine the best placement of the APs. Different AP vendors provide different tools to do this.

Site survey

To conduct a site survey, set up an AP at a particular location. Use a computer equipped with a wireless LAN device and site survey software or a handset operating in Site Survey mode to measure the strength of the signal from the AP. Move the wireless device around and repeat the measurements to determine the optimum number and best locations for the APs. This method helps identify dead zones and areas where building materials or other factors affect the performance of the network.

Site Survey mode

The handset Site Survey mode displays negative dBm levels. These levels represent the strength of the received signal (Received Signal Strength Indication or RSSI) from an AP. The RSSI information aids in determining if WLAN coverage is adequate.

For information on using the Site Survey mode, see "To test signal strength using the wireless handset" on page 103.

Note: The handsets do not require connectivity to a 2245 IP Telephony Manager or the Call Server to enable the Site Survey mode to be used. The minimum configuration required is the Extended Service Set Identifier (ESSID) of the WLAN or test AP and the WEP keys, if applicable.

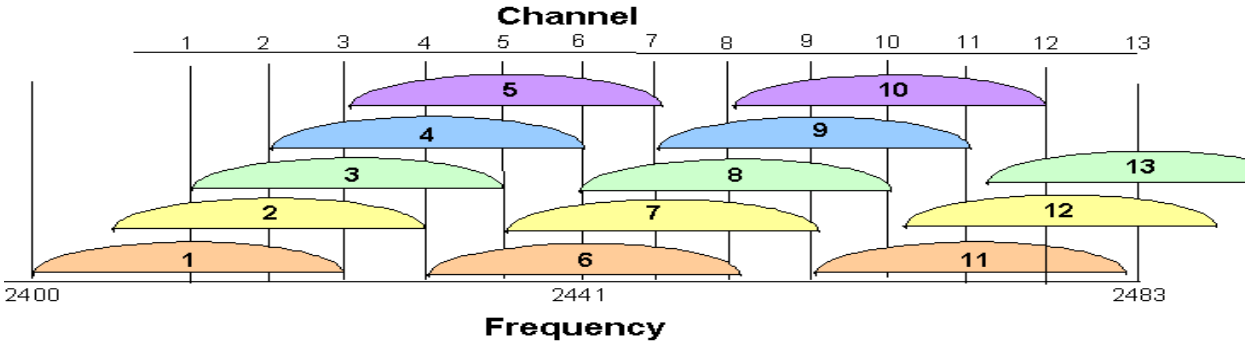
AP requirement considerations

Each site is unique in its AP requirements. Consider the following points when determining how many APs are needed and where they should be placed:

- Minimum Radio Signal Strength – All APs in the coverage area must receive a signal strength better than -70 dbm. Measurement is made in negative dbm, which measure the amount of signal loss due to distance. Therefore, stronger signals are those with smaller values. For example, -50 and -60 indicate stronger signals than -70; -80 is a weaker, poorer signal than -70.
- Adjacent APs and channel interference – In order to avoid undesirable interference from adjacent APs, ensure that adjacent APs do not use channels that overlap on the same frequencies.

Figure 1 shows the frequencies used by each channel. In the figure, channels on the same horizontal line do not overlap. In the coverage area of any given AP, signals from other APs using overlapping channels should be at least -15 to -20 dbm weaker. Because the Site Survey mode displays signals only from APs on the same Extended Service Set ID (ESSID), check for signals from APs using all ESSIDs to avoid channel overlap.

Figure 1 Frequencies used by each channel



- Wireless handset range – Wireless LAN coverage must be available wherever wireless handsets will be used. Although the typical range for a wireless handset is comparable to that of a laptop computer utilizing a wireless LAN PC card, the range may not be exactly the same. Therefore, it is preferable to use a handset to carry out the site survey, if possible. Remember that wireless handsets might be used in areas where data devices are not typically used, such as stairwells, washrooms, hallways, and outdoor areas.
- Number of wireless handsets per AP – Estimate the number of wireless handsets and the anticipated call volume per AP area to ensure that the maximum number of calls per AP will not be exceeded. See Appendix B, "Compatible Access Points for the maximum number of calls per AP for each supported manufacturer.
- The data rates at which the wireless handsets will operate – Higher data rates (such as 11Mb/s) can only be sustained while well within the range of the AP. If the wireless handsets are operating near the limits of the radio frequency (RF) coverage from the AP, they automatically drop to 1 Mb/s operation. Handsets require approximately:
  - 7% of available bandwidth per call at 11 Mb/s operation
  - 10% of the available bandwidth per call for 2 Mb/s operation
  - 15% of the available bandwidth per call for 1 Mb/s operation

Note: These requirements mean that areas with a high-use density must receive RF coverage at the highest data rate of operation.

- LAN bandwidth – Estimate anticipated peak call volume to ensure that enough bandwidth is available to handle the network traffic generated by all the wireless handsets. Handsets require approximately 150 kbps of bandwidth per call. Network traffic can be monitored/ analyzed using a network sniffer or an SNMP workstation.
- Number of other wireless devices per AP – The wireless handsets can share bandwidth with other wireless devices. To ensure adequate RF bandwidth availability, consider the number of wireless data devices in use per AP.

Note: In a very large or complex site, it may be advisable to contract a professional site survey.

Conducting an effective site survey

Consider the following points for an effective site survey.

Network usage

Examine the network usage:

- How many people will be using a wireless handset?
- What areas of the site require wireless handset access?
- How many hours each day will wireless handsets be in use?
- Which locations are likely to generate the largest amount of traffic?
- Where is future network expansion most likely?

Mobility requirements

Assess the mobility requirements:

- How many wireless handset users are in motion continually, such as in a warehouse or hospital?
- How many users work from different fixed locations throughout the site?

Physical site study

Perform a study of the physical site:

- Study blueprints of the proposed site. A site blueprint provides a map of the site, including the location of objects such as walls, partitions, and anything else that could affect the performance of a wireless handset. This helps identify areas where wireless handsets are less likely to perform well. Many obstructions are not readily visible and, in some cases, a room originally built for a specific purpose, such as a radiology lab, might have been converted into something completely different, such as a conference room. The blueprint may also show areas proposed for future building expansion.
- Mark possible wireless handset usage locations on the blueprint and refer to the marked blueprint during the physical walk-through and inventory.

Walk-through and survey

Conduct a physical walk-through and survey:

- Document any items or materials near a proposed AP location that might interfere with reception or transmission and affect wireless handset performance, such as metal shelving.
- Document stock and inventory levels, current environmental conditions, and any materials that may interfere with wireless handset transmissions.

RF transmission testing

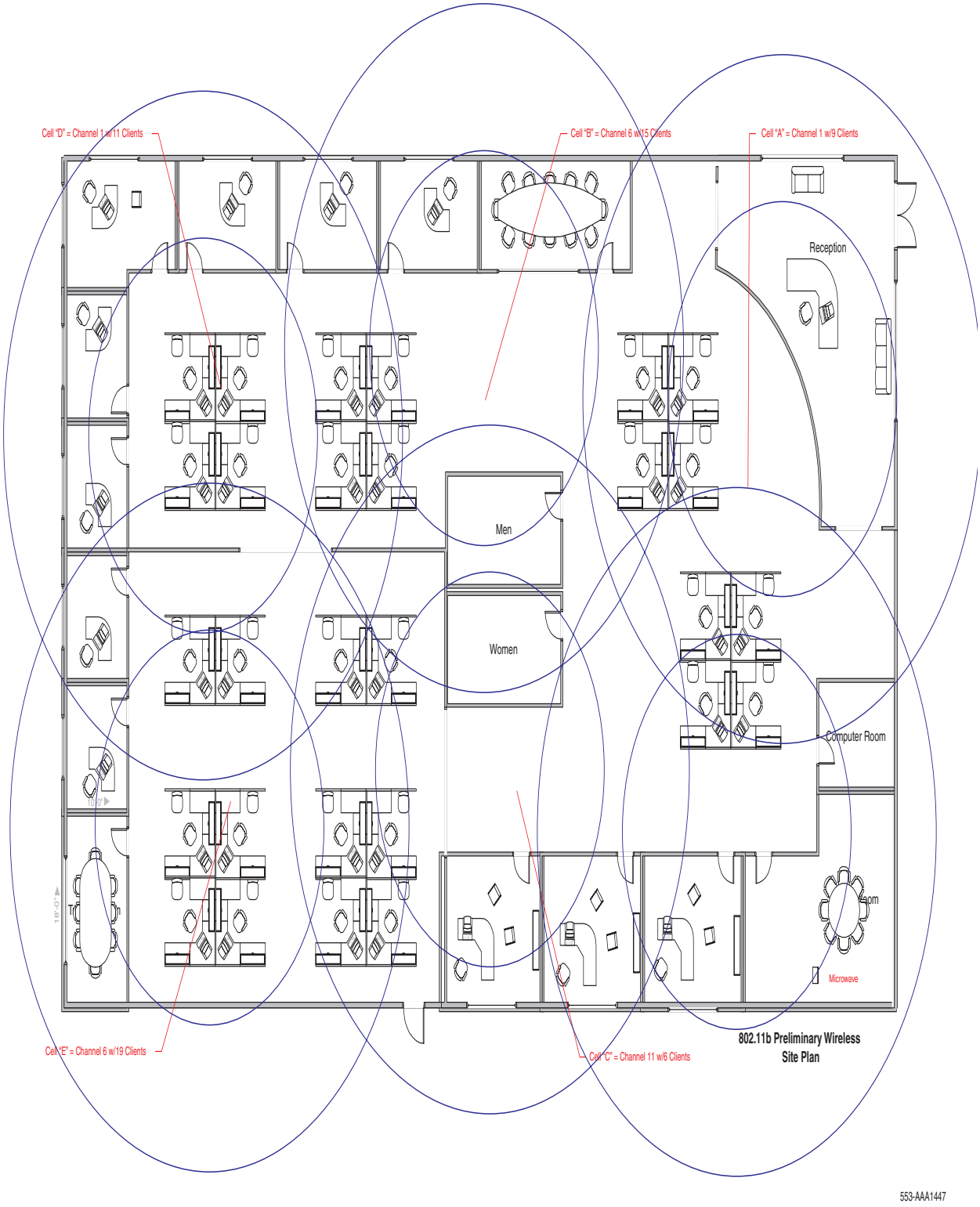
Once the APs have been installed and configured, it is necessary to measure the strength of the RF transmissions. Signal strength testing ensures that all usage areas have adequate coverage. This can be performed in two ways.

1. Use the handsets to determine AP signal strength using the Site Survey mode.
2. Use two portable computers with wireless hardware operating on a point-to-point basis. Using diagnostic software provided by the AP vendor, a coverage area for a potential AP can be determined by keeping one portable computer in one place and moving around with the other computer. Check with the vendor as to what tools are provided and what approach is recommended for deploying their APs.

Example of AP placement

Figure 2 on page 30 is an example of an AP placement diagram.

Figure 2 Sample AP placement diagram



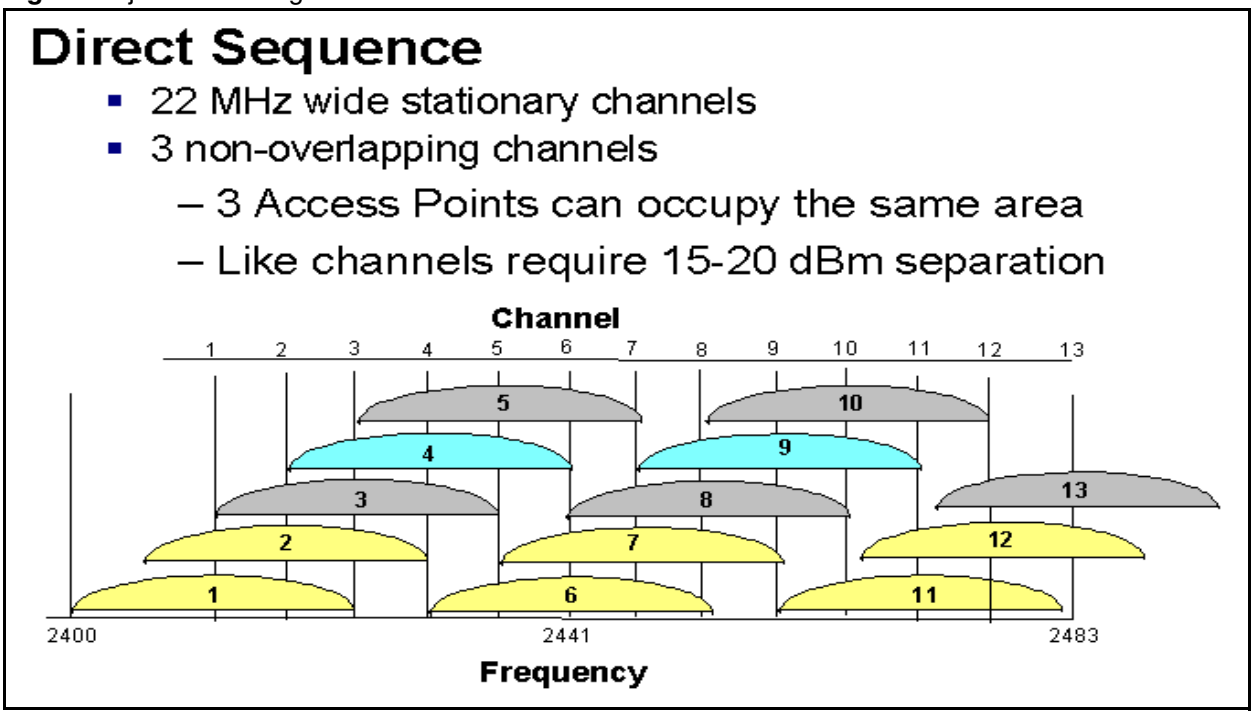
Solving coverage issues

Resolve coverage issues by adding and/or relocating APs.

Solving overlap issues

Resolve overlap issues by reassigning channels to the APs or by relocating the APs. Like channels require 15–20 dBm separation. See Figure 3.

Figure 3 jChannel assignment



Refer to the AP vendor documentation for more information on overlap.

Network planning

It is necessary to ensure that all connections and interfaces for the IP Telephony network be configured as full-duplex. Duplex mismatches anywhere on the WLAN can cause the wireless IP Telephony system not to function normally.

Zones

Nortel recommends that the handsets be assigned to dedicated zones. The zones can be used to manage the bandwidth of the WLAN IP Telephony Manager 2245 groups. As well, zone designations can be used to list the wireless handsets that are currently registered or have been registered using LD 117 commands.

For more information, see "Bandwidth management" on page 41.

WLAN IP Telephony Manager 2245 planning

Both the WLAN IP Telephony Manager 2245 and the WLAN Application Telephony Gateway 2246 are connected to the Ethernet switch.

Installation requirements

The WLAN IP Telephony Manager 2245 requires a CAT5 cable connection between its network port and the Ethernet switch. The WLAN IP Telephony Manager 2245 auto-negotiates to the type of port on the Ethernet switch. It supports 10BaseT, 100BaseT, full-duplex and half-duplex port types.

Nortel recommends 100BaseT full-duplex.

Note: When multiple WLAN IP Telephony Managers 2245 are used, all the WLAN IP Telephony Managers 2245 must use a uniform media type. Do not use full-duplex on some and half-duplex on others, or 10BaseT on some and 100BaseT on others.

Capacities

Table 3 lists the number of wireless handsets supported for the different physical media used in the network.

Table 3 Supported number of calls and wireless handsets

Media type	Number of supported calls	Number of supported wireless handsets
10BaseT	10	500
100BaseT	80	500

In any subnet where wireless handsets will be used, each subnet must have one or more WLAN IP Telephony Managers 2245. A WLAN IP Telephony Manager 2245 group on a subnet consists of one or more WLAN IP Telephony Managers 2245 and their associated wireless handsets. Only one master WLAN IP Telephony Manager 2245 can be on a subnet.

WLAN IP Telephony Manager 2245 groups

WLAN IP Telephony Manager 2245 groups are those that have more than one WLAN IP Telephony Manager 2245 in order to accommodate larger systems and a higher volume of wireless telephony traffic.

Master WLAN IP Telephony Manager 2245

In a group comprised of multiple WLAN IP Telephony Managers 2245, a master WLAN IP Telephony Manager 2245 must be identified and must be configured with a static IP address. The wireless handsets and the other WLAN IP Telephony Managers 2245 locate the master by using the master's static IP address. The loss of a non-master WLAN IP Telephony Manager 2245 does not significantly affect the operation of the remaining WLAN IP Telephony Managers 2245. However, the loss of the master WLAN IP Telephony Manager 2245 results in a loss of all communication between all the WLAN IP Telephony Managers 2245. This causes the loss of all active calls, and wireless handsets cannot check in until communication with the master is re-established.

Group capacities

Table 4 lists the capacities in a WLAN IP Telephony Manager 2245 group.

Table 4 Multiple WLAN IP Telephony Manager 2245 capacities

Number of WLAN IP Telephony Managers 2245	Calls per WLAN IP Telephony Manager 2245	Total calls	Erlangs	Number of wireless handsets 10% use	Number of wireless handsets 15% use	Number of wireless handsets 20% use
1	80	80	65	500	433	325
2	64	128	111	1000	740	‘555
3	60	180	160	1500	1067	800
4	58	232	211	2000	1407	1055
5	57	285	262	2500	1747	1310
6	56	336	312	3000	2080	1560
7	56	392	367	3500	2447	1835
8	55	440	415	4000	2767	2075
9	55	495	469	4500	3127	2345
10	55	550	524	5000	3493	2620
11	55	605	578	5500	3853	2890
12	54	648	621	6000	4140	3105
13	54	702	674	6500	4493	3370
14	54	756	728	7000	4853	3640
15	54	810	782	7500	5213	3910
16	54	874	836	8000	5573	4180

2245 Model 10 and Model 20 server capacities

The system capacity of the Model 10 and Model 20 is measured by the number of powered on handsets. If this number exceeds the maximum, the handset that cannot be served displays an error and does not connect to the SVP Server. Other handsets are not affected.

Table 5 Model 10 and Model 20 server capacities

Number of servers	Number of handsets Model 10	Number of handsets Model 20
1	10	20
2	20	40
3	30	NA
4	40	NA

Gateway and timing function

WLAN IP Telephony Managers 2245 provide both the connection, or gateway, to the Call Server for the wireless handsets, and the timing function for active calls. This gateway function is distributed across the WLAN IP Telephony Manager 2245 group.

The number of active WLAN IP Telephony Managers 2245 is determined dynamically. Whenever a WLAN IP Telephony Manager 2245 is added to or removed from the system, the distribution of timing function for active calls, as well as the gateway function, is affected.

Roaming and handover

Roaming is the ability of the wireless handset to go anywhere in the WLAN Extended Service Set RF signal coverage area, and to make and receive calls. Handover is the ability of the wireless handset to maintain an active call without interruption while moving within a WLAN ESS RF signal coverage area of a WLAN. This means that the wireless handset hands over the WLAN RF signal from AP to AP without interrupting the data stream.

APs on the same subnet

The handset can perform handover and roaming across SVP-compliant APs that reside on the same subnet as the wireless handset and WLAN IP Telephony Manager 2245 group.

APs on different subnets using WSS

When used in conjunction with a Nortel WSS 2250/2270 and Nortel APs 2230 operating in Layer 3 mode, the handsets can perform roaming and handover across APs 2230 on different subnets. The WSS 2270 operating in Layer 3 mode is on the same subnet as the WLAN IP Telephony Manager 2245 group. The WSS 2270 allows the wireless handset to retain its original IP address, whether the IP address was configured statically or obtained by DHCP. This means that roaming and handover can occur across APs 2230 placed on any subnet.

Note: The WSS 2270 must be running version 2.0.71.0 (or later) software.

Mobility across different subnets when using DHCP

If a WSS is not in use and the wireless handset IP address has been acquired through DHCP, the wireless handset must be powered down and powered up when entering a new subnet. This enables functionality of the wireless handset when entering the WLAN RF signal coverage area of a different WLAN IP Telephony Manager 2245 group on a different subnet. After the wireless handset establishes communication within the ESSID of the new WLAN, obtains another IP address from the DHCP server, and checks in with the group master, normal functionality returns. If the wireless handset is configured to use ESSID of the new WLAN, it automatically discovers the ESSID of the APs operating in broadcast mode.

Table 6 summarizes the capabilities.

Table 6 Roaming and handover capabilities summary

IP address	WSS in use	Roaming capability	Handover capability
Static	No	No	No
Static	Yes	Yes	Yes
DHCP	No	Yes, if the wireless handset is power-cycled between subnets.	No
DHCP	Yes	Yes	Yes

Multicast

IP multicast addresses are used by the WLAN Handset 2211 Push-to-talk feature. This requires that multicasting be enabled on the Layer 2 switch used by the defined group (WLAN IP Telephony Manager 2245 master/slaves and wireless handsets).

Routers are typically configured with filters to prevent multicast traffic from flowing outside of specific domains. The wireless LAN can be placed on a separate VLAN or subnet to reduce the effects of broadcast and multicast traffic from devices in other network segments.

WLAN Application Gateway 2246 planning

The optional WLAN Application Gateway 2246 requires a 10 Mb/s half-duplex switched Ethernet connection.

Installation requirements for the WLAN IP Telephony Manager 2245 and the WLAN Application Gateway 2246

Locate the WLAN IP Telephony Manager 2245 and optional WLAN Application Gateway 2246 in a space with:

- sufficient backboard mounting space and proximity to the LAN access device (switched Ethernet switch), Call Server, and power source
- rack-mount unit (if using)
- easy access to the front panel, which is used for cabling
- for the WLAN Application Telephony Gateway 2246, a maximum distance of 325 feet (100 meters) from the Ethernet switch
- for the WLAN IP Telephony Manager 2245, a maximum distance of 325 feet (100 meters) from the Ethernet switch

IP address planning

The WLAN IP Telephony Manager 2245, the optional WLAN Application Gateway 2246, and each of the wireless handsets and APs associated with them, requires an IP address.

IMPORTANT!

The master WLAN IP Telephony Manager 2245 must have an IP address statically configured.

If using DHCP for the rest of the network, the DHCP Server must have the static IP address of the master WLAN IP Telephony Manager 2245 configured on it. If using DNS, the DNS Server must have the static IP address of the master WLAN IP Telephony Manager 2245 configured on it.

The wireless handsets can be configured to use DHCP or can be assigned a static IP address. If there is no DHCP Server, the system administrator must determine what IP addresses are to be used for static addressing. As well, whether static IP addressing or DHCP is used, a pool of alias IP addresses must be configured on the WLAN IP Telephony Manager for the use of the wireless handsets. Ensure that the pool of alias IP addresses is reserved exclusively for the use of the wireless handsets.

See Chapter 6, "WLAN IP Telephony Manager 2245 configuration for information on configuring a static IP address on a WLAN IP Telephony Manager 2245. See "Configuring the WLAN Application Gateway 2246 IP address" on page 146 for information on configuring a static IP address for a WLAN Application Gateway 2246. See Chapter 7, "WLAN Handset configuration for information on configuring a static IP address on the handsets. Refer to the vendor-specific documentation for information on assigning IP addresses to the APs.

Record the static IP address assignments and store them in a safe place.

IP addressing with DHCP

A pool of alias IP addresses must be configured on the WLAN IP Telephony Manager 2245 for the use of the wireless handsets. The use of a 22-bit subnet mask provides IP addresses for approximately 500 wireless handsets (1024 nodes). Allocate a pool of an equal number of IP addresses on the DHCP server for the wireless handsets.

For example:

142.223.204.1 to 142.223.205.254 are allocated on the DHCP Server for the use of the wireless handsets.

142.223.206.1 to 142.223.207.254 are configured on the WLAN IP Telephony Manager for IP aliases for the wireless handsets.

Ensure that all these IP addresses are reserved on the DHCP Server for the use of the wireless handsets and not assigned to any other device.

Planning worksheets

Complete this worksheet and the worksheet in Table 8 on page 39 before beginning the installation.

Copy and complete this worksheet in Table 7 for each WLAN IP Telephony Manager 2245. Obtain the necessary information from the network administrator.

Table 7 WLAN IP Telephony Manager 2245 planning worksheet

Unit number	
IP address	
Hostname	
Subnet Mask	
Default Gateway	
Master WLAN IP Telephony Manager 2245	
TFTP Download Master IP address	
Primary DNS Server IP address	

Table 7 WLAN IP Telephony Manager 2245 planning worksheet

Secondary DNS Server IP address	
DNS Domain	
WINS Server IP address	
Workgroup name	
Syslog Server IP address	
First alias IP address	
Last alias IP address	

Copy and complete this worksheet in Table 8 to maintain a configuration record for the handsets.

Table 8 Wireless handset planning worksheet

Line *	MAC Address *	User Name	Dialing Ext.	IP Address (if statically configured)
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
* – required only if using the optional WLAN Application Gateway 2246.				

Chapter 4
System information

Bandwidth management

Bandwidth management using bandwidth zones applies to the handsets.

Zones

A WLAN IP Telephony Manager 2245 group consists of a master WLAN IP Telephony Manager 2245, zero to 15 WLAN IP Telephony Manager 2245 slaves, and their associated wireless handsets.

It is good practice to create a Bandwidth Management Zone for each WLAN IP Telephony Manager 2245 group (one group per subnet) in LD 117. Use the **CHG ZDES** command to name the zone with the IP address of the master WLAN IP Telephony Manager 2245.

=> **NEW ZONE** <zone number>

=> **CHG ZDES** <zone number> <Wnnn.nnn.nnn.nnn>
where W indicates “WLAN IP Telephony Manager 2245” and nnn.nnn.nnn.nnn is the IP address of the master WLAN IP Telephony Manager 2245.

=> **PRT ZDES ALL**

This allows the system administrator or support personnel to print a list of the IP addresses of all the master WLAN IP Telephony Managers 2245 in the system simply by printing the Zone designators in LD 117. They are printed as Wnnn.nnn.nnn.nnn. This enables support personnel to easily obtain the IP address of a WLAN IP Telephony Manager 2245 so they can telnet to the WLAN IP Telephony Manager 2245 in order to diagnose and correct problems.

Zones for wireless handsets

Assign the virtual line TNs for the wireless handsets (configured in LD 11) to the zone number assigned to its home WLAN IP Telephony Manager 2245 group. Using LD 117, this enables support personnel to list the current registration status of all wireless handsets that belong to the zone of a specific WLAN IP Telephony Manager 2245 group.

=> **STIP ZONE** <zone number>

All wireless handsets currently registered (checked in) with their home WLAN IP Telephony Manager 2245 group will be listed. The format of the list is **TERMIP** = <alias IP address>, which is located in the same subnet as the IP address of the master WLAN IP Telephony Manager 2245 of the group. Any wireless handsets that are currently checked in with another WLAN IP Telephony Manager 2245 group are listed with a TERMIP in a different subnet from that of their home WLAN IP Telephony Manager 2245 group ZDES.

Current registration status of wireless handsets

To list the current registration status of all wireless handsets that are registered in a specific subnet, regardless of their home zone, use either of the following LD 117 commands.

STIP TERMIP <subnet of the WLAN IP Telephony Manager 2245 group>

or

PRT IPDN <subnet of the WLAN IP Telephony Manager 2245 group>

Alias IP address

Using the DN of a wireless handset, support personnel can obtain the current or most recent alias IP address used by a wireless handset when it checked in with the master of a WLAN IP Telephony Manager 2245 group, and subsequently registered with the LTPS and Call Server.

=> **PRT DNIP** <DN of wireless handset>

Designating wireless telephone types

Unless there is another preferred use for the DES (Designator) prompt in LD 11, Nortel recommends using the DES prompt to indicate the type of WLAN Handset — either type 2210, 2211, or 2212 — for the i2004 type of virtual line TN. This allows support personnel to enter 2210, 2211, or 2212 at the LD 20 DES prompt and receive a list of handsets that are configured on the Call Server.

Call blocking

The WLAN IP Telephony Manager 2245 controls the media stream and blocks calls due to bandwidth constraints on any AP without notifying the Call Server.

- The WLAN IP Telephony Manager 2245 can be configured with the maximum number of simultaneous calls allowed on a single AP.
- On an incoming call for a wireless handset associated with a full AP, the caller hears ringback and the Call Forward No Answer (CFNA) treatment is applied, such as forwarding the call to voicemail. The called party is not notified of the incoming call.
- If the call originates from a wireless handset that is on a bandwidth-restricted AP, the caller hears a warning tone and the call is blocked.
- If a wireless handset moves into an area serviced by an AP that is already at capacity, the wireless handset will not associate with the new AP. Instead, the wireless handset attempts to remain associated with an AP that has sufficient bandwidth. This could result in packet loss, degraded signal and voice quality, and a call could be dropped.
- UNIStim signaling, such as watchdog updates or lamp audit, are not affected by the bandwidth constraint.

Codecs

G.711, G.729A, and G.729B codecs are supported. The RTP packets that transit between the wireless handsets and the WLAN IP Telephony Manager 2245 always contain 30 msec of voice. The WLAN IP Telephony Manager 2245 repackages the voice data to the correct packet size. The jitter buffer is always configured to 70 msec, and any UNIStim messages that configure the jitter buffer are ignored.

IMPORTANT!

If the wireless handset is registered to the same LTPS as the IP Phones, then configure only the subset of codecs supported by both the wireless handsets and the IP Phones.

If it is necessary for the IP Phone to use a codec that is not supported on the wireless handsets, such as G.723.1, then the wireless handsets must be configured on their own separate node.

If a remote endpoint is configured for G.723.1 as the Bbest Bandwidth (BB) Codec and G.711 as the Best Quality (BQ) Codec, (G.729 is not configured), the media path negotiates to G.711. The result may be unexpected consequences on a narrow-band link.

Jitter buffer

The handsets do not support a configurable jitter buffer. If they receive the “Jitter Buffer Configuration” UNIStim message, the command is ignored. The jitter buffer is fixed at 70 msec.

There are two implications of a fixed jitter buffer setting:

- If the system jitter buffer setting is less than 70 msec (default is 50 msec), there is a slightly longer delay in the IP Phone receive direction.
- If the system jitter buffer setting is longer than 70 msec to accommodate severe network jitter, there could be slightly higher packet loss in the IP Phone receive direction.

The longer than normal jitter buffer setting is reasonable since extra jitter is introduced by the RF portion of the link.

RLR and SLR

The handsets do not support UNIStim messages used to adjust the Receive Loudness Rating (RLR) and Send Loudness Rating (SLR) of the wireless handset.

RTCP

Handsets do not support Real-time Transport Control Protocol (RTCP). Incoming RTCP packets sent to the wireless handsets are actually sent to the WLAN IP Telephony Manager 2245 and are discarded. If the wireless handset is queried for RTCP parameters, the wireless handset returns dummy values of 0 jitter, 0 latency, and 0 packet loss.

Gain adjustment

The handsets ignore any UNIStim messages that adjust the loss plan of the wireless handset.

Programmable rings and tones

The wireless handsets support alerting cadences but only a single alerting frequency.

The wireless handsets have the same call progress tone capability as the existing IP Phones 2004.

In/Out of Service tones

When the handset completes registration with the Call Server, it plays the “In Service” tone. When the handset loses connection with the Call Server and re-sets, it plays the “Out of Service” tone.

Local mode display

Because the default state of the wireless handset is Standby, it is only possible to determine if the wireless handset is in Local mode by pressing the off-hook (Green) or the MENU keys. Pressing these keys changes the state of the handset to Active Idle or Active Off-Hook, therefore putting it in communication with the primary Signaling Server.

For the MG 1000B, if a wireless handset is registered to the Small System Controller (SSC) in Local mode, then the local-mode license information is displayed on the wireless handset on the second line of the display. Since the maximum number of display characters on the wireless handset is 19 characters, the local-mode license information on the wireless handset display is truncated. See Table 9.

Table 9 IP Phone 2004 and handset Local mode license display (MG 1000B only)

IP Phone 2004	Handset
Licensed days left x	Licensed days lft x
Licensed days left xx	Licensed ds lft xx
Beyond licensed period	Beyond licensd prd

Survivable Remote Gateway

The handset can be deployed in a Survivable Remote Gateway (SRG) configuration for both SRG 1.0 and SRG50.

Test Local mode is not accessible because the Services key is not supported in Local mode.

The navigation keys are supported in Normal mode and not in Local mode.

Since the default state of the wireless handset is Standby, it is only possible to determine if the wireless handset is in Local mode by pressing the off-hook (Green) or MENU keys. Pressing these keys changes the state of the handset to Active Idle or Active Off-Hook, therefore putting it in communication with the primary Signaling Server in the main office.

Note: In order to allow SRG 1.0 systems based on BCM 3.6, to correctly operate with the handsets, they must have a software patch installed. The patch can be downloaded from the Nortel Electronic Software Delivery web site.
The BCM/SRG 3.6 WLAN IP Telephony Feature patch is called BCM_360[1].039__WLAN_IP_Telephony_Patch.exe, which includes 51 files required for automated patch installation.

Note: No patch is required for SRG 1.0 based on BCM 3.7 or SRG50 systems

External Applications Server

The External Applications Server (XAS) applications are not available on the handsets.

End-to-end QoS

End-to-end QoS, such as DiffServ, and Layer 2 QoS, such as 802.1 Q/p, are not supported on the wireless telephone system. Any UNIStim commands sent to the wireless handsets attempting to adjust Layer 2 or Layer 3 QoS parameters are ignored. In addition, the WLAN IP Telephony Manager 2245 does not support any Layer 2 or Layer 3 QoS mechanisms.

However, it is possible to provide QoS mechanisms through configuration of network equipment.

The Layer 2 switch port to which the WLAN IP Telephony Manager 2245 is connected can be configured to add 802.1 Q/p tagging. The Layer 3 port that acts as the gateway for the WLAN IP Telephony Manager 2245 can be configured to add the appropriate DiffServ tagging. Since all of the signaling and media traffic passes through the WLAN IP Telephony Manager 2245, all packets are tagged with the appropriate priority. If more than one WLAN IP Telephony Manager 2245 is used, each Layer 2 port to which a WLAN IP Telephony Manager 2245 is connected must be configured to add the 802.1 Q/p tagging.

NAT

If external or third party NAT (Network Address Translation) is employed, the BCM, the APs and handsets, and the 2245, must all reside on the same side of the NAT. Either all must be on the public network side or all on the private network side.

IP Phone 2004 features

Table 10 provides information on the IP Phone 2004 features for the handsets.

Table 10 IP Phone 2004 features

Feature	Supported on the handsets	Description
Keypad	Yes	
Navigation keys	Yes	Up — Volume Up button Down — Volume Down button Left — button Right — button
6 feature keys	Yes	
4 soft-labelled keys	Yes	
Display	Partially	IP phone 2004: 5x24 display Handsets: 4x19 display
Message Waiting Indicator	Yes	Small envelope icon (I) in the top right of the handset LCD display
Branch Office	Yes	
Survivable Remote Gateway	Yes	
Virtual Office	Partially	No “Services” key. Use FCN+7 for the Services key to support Virtual Office.
XAS	No	No “Expand” key.
Personal Directory Callers List Redial List	Yes	
Password Admin	No	The handsets can be password-protected, but this is different from the IP Phone 2004 password protection mechanism. The IP Phone 2004 password protection is supported, in addition to the handset password protection.
KEM	No	

Chapter 5
Installation

Required materials

The following equipment must be provided by the customer:

- power outlet(s) – must accept the provided AC adapter, one for the WLAN IP Telephony Manager 2245 and one for the WLAN Application Gateway 2246 (if used).
- plywood backboard space – the WLAN IP Telephony Manager 2245 is designed to be wall-mounted to ¾" plywood securely screwed to the wall.
  or
  optional WLAN IP Telephony Manager 2245 rack-mount kit (must be ordered separately), containing mounting plates and screws
- screws – used to mount the WLAN IP Telephony Manager 2245 to the wall. Four #8 - ¾" panhead wood screws (or similar devices) are required.
- 10BaseT CAT5 cable with an RJ-45 connector for the optional WLAN Application Gateway 2246 – provides a connection to the Ethernet switch.
- CAT5 cable with an RJ-45 connector for the WLAN IP Telephony Manager 2245 – provides a connection to the Ethernet switch.
- DB-9 female null-modem cable – required for initial configuration of the WLAN IP Telephony Manager 2245 and WLAN Application Gateway 2246.

Supplied equipment

Each WLAN IP Telephony Manager 2245 and WLAN Application Gateway 2246 is shipped with one Class II AC adapter with 24V DC, 1A output.

Pre-installation checklist

Ensure that the following requirements have been met prior to installation:

- The location chosen for the WLAN IP Telephony Manager 2245 and WLAN Application Gateway 2246 is adequate and power is available.
- APs are SVP-compatible and coverage is adequate.
- A dedicated line is available for remote modem access, if needed.
- The telephone system administrator is on-site to program the existing telephone system.

Installing the WLAN IP Telephony Manager 2245

The following are the tasks that must be completed to install the WLAN IP Telephony Manager 2245:

1 "Wall mounting" on page 49.
or
"Rack-mounting" on page 49.

2 "Connecting to the LAN" on page 50.

3 "Connecting to the power" on page 50.

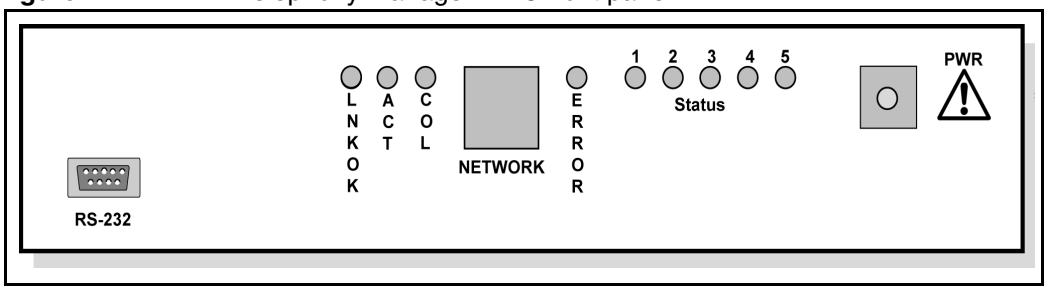
About the front panel

The front panel of the WLAN IP Telephony Manager 2245 contains ports to connect to the following:

- power
- LAN
- administrative computer through an RS-232 port

Status LEDs supply information about the WLAN IP Telephony Manager 2245's status and activity. See Figure 4.

Figure 4 WLAN IP Telephony Manager 2245 front panel



- **RS-232** port – the male DB-9 connector (DTE). Provides an RS-232 connection to a terminal, terminal emulator, or modem for system administration.
- Link LEDs
  - **LNKOK** – lit when there is a network connection
  - **ACT** – lit when there is system activity
  - **COL** – lit if there are network collisions
- **NETWORK** – connects the WLAN IP Telephony Manager 2245 to the wired Ethernet LAN
- **ERROR** LED – lit when the system has detected an error

- **Status** LEDs – indicate system error messages and status
  - **1** – heartbeat
  - **2** – active calls
  - **3, 4, 5** – currently unused
- **PWR** – connects to the AC adapter supplying power to the system

WARNING

Use only the provided Class II AC adapter with 24V DC, 1A output.

Wall mounting

The WLAN IP Telephony Manager 2245 can be mounted either vertically or horizontally.

To wall-mount the WLAN IP Telephony Manager 2245

1. Use a 1/8-inch drill bit to drill four pilot holes, on 1.84 by 12.1 inch centers (approximately equivalent to 1-13/16 inch by 12-1/8 inch).
2. Insert the #8 x 3/4-inch screws in the pilot holes and tighten, leaving a 1/8 to 1/4-inch gap from the wall.
3. Slide the WLAN IP Telephony Manager 2245 over the screws until the WLAN IP Telephony Manager 2245 drops into place in the keyhole openings of the flange.
4. Tighten screws fully.

Rack-mounting

The rack-mount kit is designed for mounting the WLAN IP Telephony Manager 2245 in a standard 19-inch rack and contains the following equipment:

- Mounting plates – two for each WLAN IP Telephony Manager 2245 to be mounted.
- Screws – four rack-mount screws for each WLAN IP Telephony Manager 2245 to be mounted.

To rack-mount the WLAN IP Telephony Manager 2245

1. Remove the corner screws from the WLAN IP Telephony Manager 2245.
2. Screw the U-shaped end (round screw holes) of the two mounting plates to the WLAN IP Telephony Manager 2245.
3. Screw the other end of the two mounting plates (oblong screw holes) to the rack.
4. Repeat steps 1-3 for each additional WLAN IP Telephony Manager 2245. The mounting plate is designed to provide the correct minimum spacing between units. When mounting multiple units, stack the units in the rack as closely as possible.

Connecting to the LAN

Use an RJ-45 cable to connect the NETWORK port on the WLAN IP Telephony Manager 2245 to the connecting port on the Ethernet switch.

Connecting to the power

Follow the steps in the following procedure to connect the power to the WLAN IP Telephony Manager 2245.

To connect the power

1. Connect the power plug from the AC adapter to the jack labeled **PWR** on the WLAN IP Telephony Manager 2245.

WARNING

Use only the provided Class II AC adapter with output 24V DC, 1A.

2. Plug the AC adapter into a 110V AC outlet to supply power to the WLAN IP Telephony Manager 2245.

   The system cycles through diagnostic testing and the LEDs blink for approximately one minute.

3. When the system is ready for use, verify the following:
   a. **ERROR** LED is off.
   b. **Status 1** is blinking.

Installing the WLAN Application Gateway 2246

For information on installing the optional WLAN Application Gateway 2246, see Appendix A, “WLAN Application Gateway 2246.

Chapter 6
WLAN IP Telephony Manager 2245 configuration

The WLAN IP Telephony Manager 2245 acts as a proxy for the wireless handsets and provides several services for them. It is connected to the same subnet as the wireless handsets. The wireless handsets always communicate voice and signaling directly with the WLAN IP Telephony Manager 2245, using the proprietary SVP protocol.

SVP is required for QoS because the current IEEE 802.11a/b/g wireless LAN standard provides no mechanism for differentiating audio packets from data packets. This standard is undergoing revision to version 802.11e to provide functionality in an industry standard similar to SVP, therefore ensuring high-quality voice in a mixed-client environment.

Functional description

- The WLAN IP Telephony Manager 2245 provides the following services to the handsets:
- It acts as a proxy for every wireless handset; that is, all UNIStim signaling and RTP media to/from the wireless handset pass through the WLAN IP Telephony Manager 2245. Except for the initial DHCP and TFTP sessions, the wireless handsets only communicate with the WLAN IP Telephony Manager 2245.

  Each WLAN IP Telephony Manager 2245 is configured with an IP address with which all of the wireless handsets communicate. In addition, each WLAN IP Telephony Manager 2245 is configured with a pool of IP addresses. When a wireless handset registers with a WLAN IP Telephony Manager 2245, the wireless handset is assigned one of the IP addresses from the pool. All communication between this WLAN IP Telephony Manager 2245 and other devices (TPS, IP Phones, gateways, and other wireless handsets) is always done through its pool IP address. In this sense, the WLAN IP Telephony Manager 2245 acts as a NAT (Network Address Translation).

Note: The WLAN IP Telephony Manager 2245 has a single physical Ethernet interface and MAC address; therefore, all of the IP addresses are mapped to a single MAC address.

- The WLAN IP Telephony Manager 2245 server tags/untags packets with the SVP header. SVP packets have the protocol byte of the IP header set to 0x77. SVP-compliant APs use this proprietary tagging to give priority to tagged packets. For UDP (UNIStim and RTP) packets going from the wireless handset to the network, the WLAN IP Telephony Manager 2245 replaces the SVP protocol number, 0x77, with the UDP number, 0x11. For packets going from the network to the wireless handset, the protocol number is changed from 0x11 to 0x77.

  Because packets that traverse the network between the wireless handset and the WLAN IP Telephony Manager 2245 are not standard IP packets (the packets use a non-standard protocol number), there can be no Layer 3 routing in the path. Therefore, the wireless handsets and WLAN IP Telephony Managers 2245 must be in the same logical subnet.
- RTP packets between the wireless telephone and the WLAN IP Telephony Manager 2245 always contain 30 ms worth of voice, no matter what has been configured on the Call Server. The WLAN IP Telephony Manager 2245 repackages the RTP packets to conform to the size that has been configured in the Call Server. This provides more efficient use of the available Radio Frequency (RF) bandwidth at the expense of slightly increased jitter and latency.
- The WLAN IP Telephony Manager 2245 is configured with a maximum allowable number of simultaneous media streams on a single AP. The WLAN IP Telephony Manager 2245 keeps track of the number of media streams on each AP and blocks calls to/from a wireless handset that would exceed the configured capacity. For more information on call blocking, see “Call blocking” on page 42.

  A keep-alive packet exchange runs between the wireless handset and the WLAN IP Telephony Manager 2245 every 30 seconds. If the wireless handset detects that the WLAN IP Telephony Manager 2245 is unreachable, the wireless handset resets itself and attempts to re-establish a connection with the master WLAN IP Telephony Manager 2245.

Configuration tasks

To configure the WLAN IP Telephony Manager 2245

1. “Connecting to the WLAN IP Telephony Manager 2245” on page 53.
2. “Configuring the network” on page 55.
3. “Configuring the WLAN IP Telephony Manager 2245” on page 58.
4. “Changing the password” on page 61.

In the initial configuration of the WLAN IP Telephony Manager 2245, the IP addresses and the maximum number of active calls per AP must be configured. Later, the IP address of the TFTP Server where the software files are located and the hostname can be configured by Telnet.

Connecting to the WLAN IP Telephony Manager 2245

The initial connection to the WLAN IP Telephony Manager 2245 must be made through a serial connection to establish the WLAN IP Telephony Manager 2245 IP address. After the IP address is established, connection to the WLAN IP Telephony Manager 2245 can be done through the network using Telnet.

Nortel recommends that the complete initial configuration be performed when the serial connection is made.

Through a serial port

Follow the steps in Procedure to connect to the WLAN IP Telephony Manager 2245 through a serial port.

To connect to the WLAN IP Telephony Manager 2245 through a serial port

1. Using a DB-9 female, null-modem cable, connect the WLAN IP Telephony Manager 2245 to the serial port of a terminal or PC.
2. Run a terminal emulation program (such as HyperTerminal), or use a VT-100 terminal with the following configuration:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

Note: If using Windows 2000, Service Pack 2 must be installed to enable the use of HyperTerminal.

3. Press **Enter** to display the login screen.
4. Enter the default login **admin** and the default password **admin**.

Note: The login name and password are case-sensitive.

The NetLink SVP-II System screen displays. See Figure 5 on page 54.

Through Telnet

The Telnet method of connection is used for routine maintenance of the WLAN IP Telephony Manager 2245 for local and remote administration, depending on the network.

Note: Telnet can only be used after the WLAN IP Telephony Manager 2245 IP address is configured.

To connect to the WLAN IP Telephony Manager 2245 through Telnet

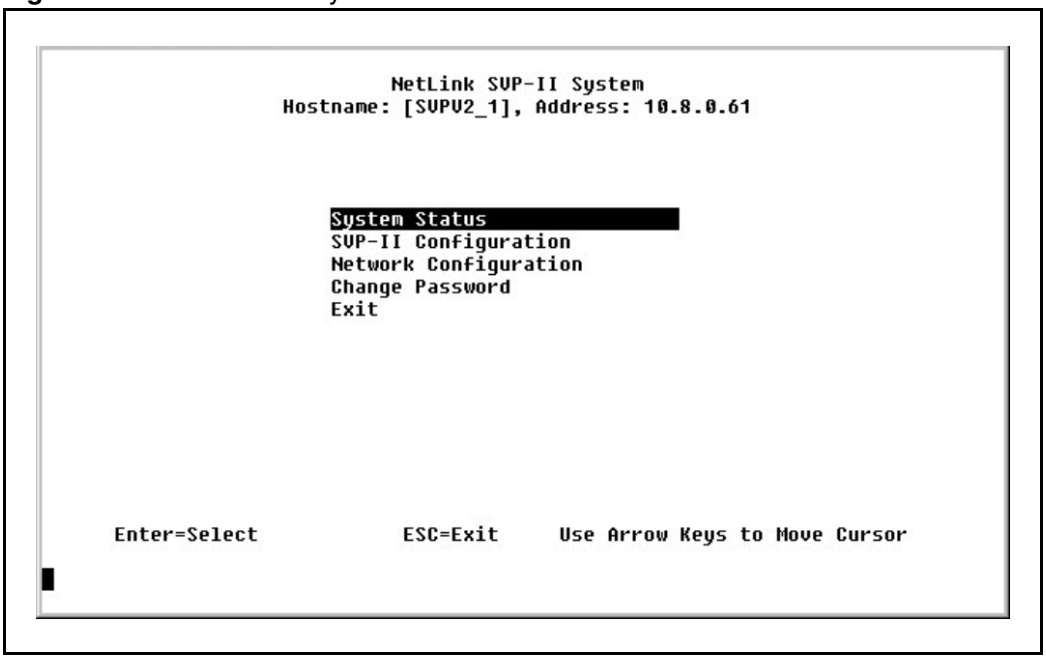
1 Run a Telnet session to the IP address of the WLAN IP Telephony Manager 2245.

2 Enter the login and the password.

Note: The login name and password are case-sensitive.

The **NetLink SVP-II System** menu displays. See Figure 5 on page 54.

Figure 5 NetLink SVP-II System screen



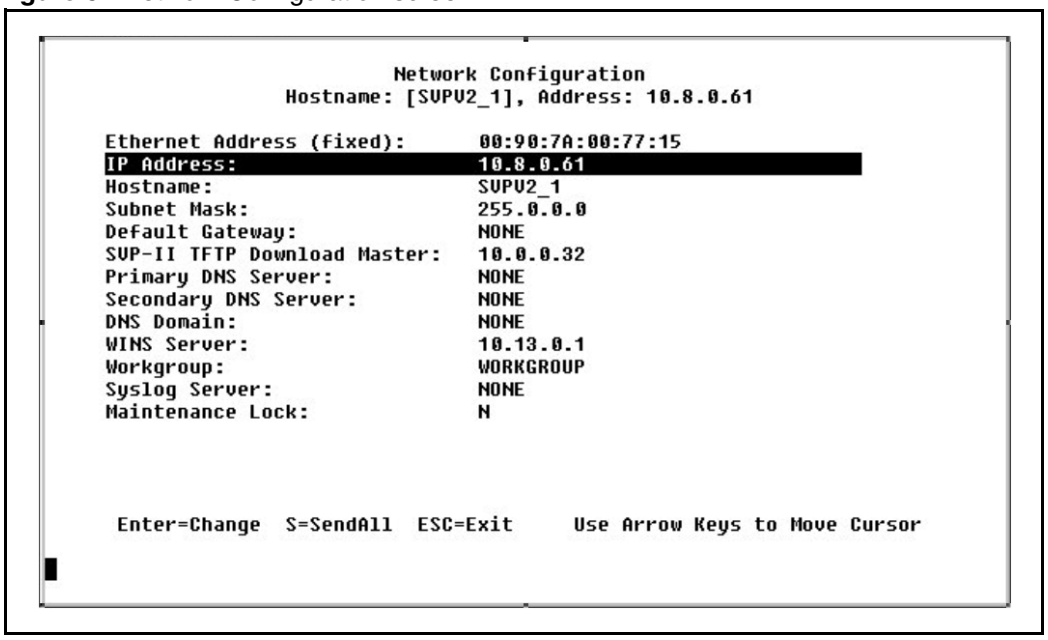
The following menu choices are available:

- **System Status** – view software code version, error messages, and status of operation. See "To view the software version" on page 111 and Chapter 9, "Troubleshooting.
- **SVP-II Configuration** – set the mode and reset the system. See "Configuring the WLAN IP Telephony Manager 2245" on page 58.
- **Network Configuration** – set network configuration options, including IP addresses and hostname. See "Configuring the network" on page 55.
- **Change Password** – change the password for WLAN IP Telephony Manager. See "Changing the password" on page 61.
- **Exit** – exit the menu.

Configuring the network

Select **Network Configuration** on the **NetLink SVP-II System** screen to configure the IP address and other network settings of the WLAN IP Telephony Manager 2245. An optional Hostname and the IP address of TFTP Server containing the software update files are also configured here. The Network Configuration screen is shown in Figure 6.

Figure 6 Network Configuration screen



Configure the following fields with information provided by the network administrator:

- **IP Address:** – enter the complete IP address for the WLAN IP Telephony Manager 2245, including digits and periods.

Note: If this WLAN IP Telephony Manager 2245 is the master, it must have a static IP address configured. Do not use DHCP to assign the IP address of the master WLAN IP Telephony Manager 2245. Other WLAN IP Telephony Managers 2245 in a multiple WLAN IP Telephony Manager 2245 environment can have their IP address assigned by DHCP.

Fore more information on the master WLAN IP Telephony Manager 2245, see "WLAN IP Telephony Manager 2245 planning" on page 32.

- **Hostname**: – optional field. Change the default hostname of this WLAN IP Telephony Manager 2245, if desired. Hostname is for identification purposes only.

Note: Spaces cannot be entered in this field.

- Subnet mask – the subnet mask of the subnet.
- **Default Gateway** – the default gateway for the subnet.
- **SVP-II TFTP Download Master** – the IP address of the TFTP Server where the software update files are saved. Enter one of the following:
  - **NONE** – disables this function
  - IP address of the TFTP Server that transfers software updates to the WLAN IP Telephony Manager 2245

- **Primary DNS Server, Secondary DNS Server, DNS Domain** – used to configure Domain Name Services (DNS). Obtain the settings from the network administrator. Optionally, enter **DHCP**. This enables the DHCP client in the WLAN IP Telephony Manager 2245 to attempt to automatically obtain a valid IP address from the DHCP Server. The DHCP setting is only valid when the IP address is obtained from DHCP.
- **WINS Server** – the IP address of the Windows Name Services (WINS) Server. Obtain the settings from the network administrator.

  Optionally, enter **DHCP**. This enables the DHCP client in the WLAN IP Telephony Manager 2245 to attempt to automatically obtain a valid IP address from the DHCP Server. The DHCP setting is only valid when the IP address is obtained from DHCP.

  When WINS is configured, the WLAN IP Telephony Manager 2245 can translate hostnames to IP addresses. This means that when using Telnet, the WLAN IP Telephony Manager 2245 can be accessed using its hostname rather than its IP address.
- **Syslog Server** – the IP address of the server where the system logs for the WLAN IP Telephony Manager 2245 are written. If a Syslog Server is configured, a message is sent to the Syslog Server when an alarm is generated. Enter one of the following:
  - **NONE** – disables this function
  - IP address of the Syslog Server
- **Maintenance Lock** – indicates if the WLAN IP Telephony Manager 2245 is in Maintenance Lock mode.
- **SendAll** – in a system with multiple WLAN IP Telephony Managers 2245, the SendAll option is provided to speed configuration and ensure identical settings. The S=SendAll option enables configuration parameters of the selected field to be sent to every WLAN IP Telephony Manager 2245 on the LAN. SendAll can only be used after the IP address is configured on each WLAN IP Telephony Manager 2245 using a serial connection. If identical configuration parameters are to be used for all WLAN IP Telephony Managers 2245, configure only the IP address and custom hostname (if desired) on each WLAN IP Telephony Manager 2245 using the initial serial connection. Then connect through the LAN to this WLAN IP Telephony Manager 2245 and use SendAll to transmit identical configuration options of each field for all WLAN IP Telephony Managers 2245.

IMPORTANT!

If SendAll is used on the system, all passwords must be identical. Do not change the password at the initial configuration if the SendAll option will be used. Use the default password and change it globally, if desired, after a LAN connection is established for all WLAN IP Telephony 2245 units.

If independent administration of each WLAN IP Telephony Manager 2245 is desired, the passwords can be set during initial configuration.

Saving the configuration

Reset the WLAN IP Telephony Manager 2245 in order to save the configuration parameters.

To save the configuration

1. Press **Esc** on the keyboard.

   If the WLAN IP Telephony Manager 2245 is in **Maintenance Lock**, a prompt appears asking if the configuration is to be saved.

2. Enter **Y**.

3. Alternatively, select the **Reset** option found in the **SVP-II Configuration** screen. Press **Esc**.

   See "Configuring the WLAN IP Telephony Manager 2245" on page 58.

Changing the master IP address

To change the IP address of the master WLAN IP Telephony Manager 2245, change it in the Network Configuration menu and reboot the system. Then alias IP addresses can be changed in each of the other WLAN IP Telephony Managers 2245 without incurring an error.

Configuring the WLAN IP Telephony Manager 2245

The WLAN IP Telephony Manager 2245 is configured on the SVP-II Configuration screen where the mode of the WLAN IP Telephony Manager 2245 is configured. This screen is also used to lock the WLAN IP Telephony Manager 2245 for maintenance and reset the WLAN IP Telephony Manager 2245 after maintenance.

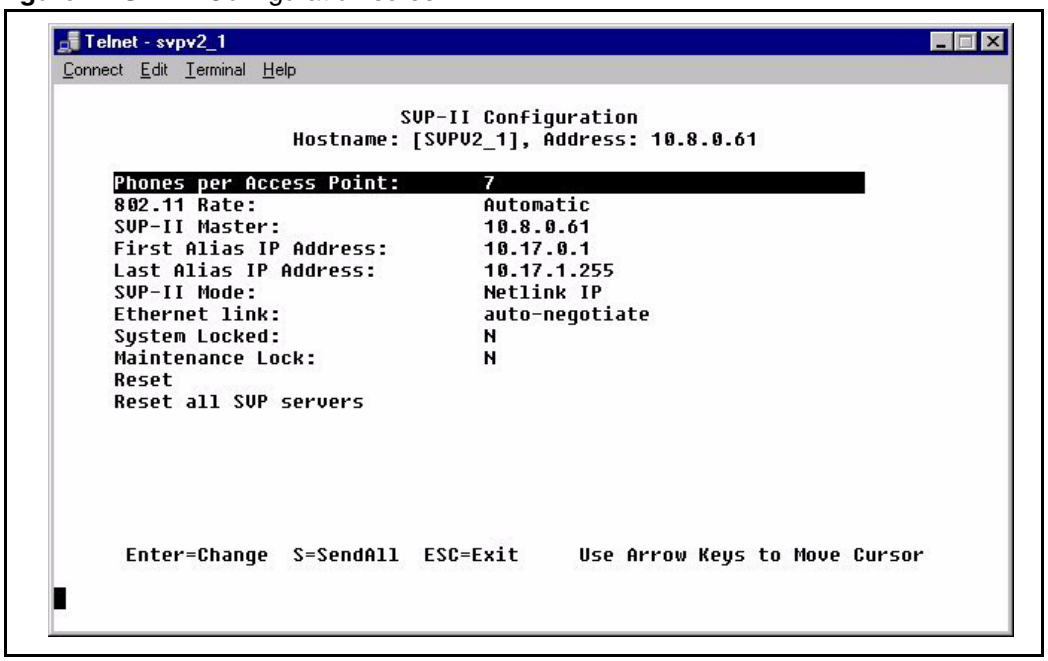
The WLAN IP Telephony Manager 2245 automatically locks for maintenance if the IP address is changed. When a Maintenance Lock occurs, the WLAN IP Telephony Manager 2245 must be reset upon exit. All active calls are terminated during a reset.

Access the SVP-II Configuration screen from the NetLink SVP-II System menu. Scroll to SVP-II Configuration and press Enter.

The SVP-II Configuration screen is shown in Figure 7 on page 59.

Perform the desired SVP-II configuration.

Figure 7 SVP-II Configuration screen



- **Phones per AP** – enter the number of simultaneous calls supported for the AP type. AP specifications are described in Appendix B, "Compatible Access Points.
- **802.11 Rate** – select **Automatic** to allow the wireless handset to determine its rate (up to 11Mb/s). Select **1MB/2MB** to limit the transmission rate between the wireless handsets and APs.
- **SVP-II Master** – the IP address of the master of the WLAN IP Telephony Manager 2245 group must be identified. Select one of the following identification options:
  - Enter the IP address of the master of the WLAN IP Telephony Manager 2245 in each WLAN IP Telephony Manager 2245 group. Include the periods used in the IP address.
  - Enter **DHCP**. Ensure that the IP address of the master WLAN IP Telephony Manager 2245 has been configured in the DHCP server and configure the other WLAN IP Telephony Managers 2245 to obtain the information from the DHCP server.
  - Enter **DNS**. Ensure that the IP address of the master WLAN IP Telephony Manager 2245 has been configured in the DNS server and configure the other WLAN IP Telephony Managers 2245 to retrieve this information from the DNS server.
- First Alias IP Address / Last Alias IP Address – enter the range of IP addresses that this WLAN IP Telephony Manager 2245 can use when acting as a proxy for the wireless handsets.

Note: All alias addresses must be on the same subnet as the WLAN IP Telephony Manager 2245. The IP addresses cannot be duplicated on other subnets or WLAN IP Telephony Managers 2245. There is no limit to the number of IP addresses that can be assigned, but the capacity of each WLAN IP Telephony Manager 2245 is 500 wireless handsets.

- **SVP-II Mode** – select NetLink IP.

- **Ethernet link** – select auto-negotiate unless there is a need to specify the link speed.
- **System Locked** – use this option to take the system down for maintenance. The default is **N** (No). Select **Y** (Yes) to prevent any new calls from starting. Enter N to restore normal operation.
- **Maintenance Lock** – the system automatically sets this option to Y (Yes) after certain maintenance activities that require a reset are performed, such as changing the IP address. Maintenance Lock prevents any new calls from starting. This option cannot be changed. It is automatically set by the system. Reset the WLAN IP Telephony Manager 2245 at exit to clear Maintenance Lock.
- **Reset** – if this option is selected, a prompt appears to reset the WLAN IP Telephony Manager 2245 when exiting the SVP-II Configuration screen.
- **Reset all SVP servers** – if this option is selected, all WLAN IP Telephony Managers 2245 on the subnet are reset.

Note: Resetting the WLAN IP Telephony Manager 2245 terminates any calls in progress.

Changing the password

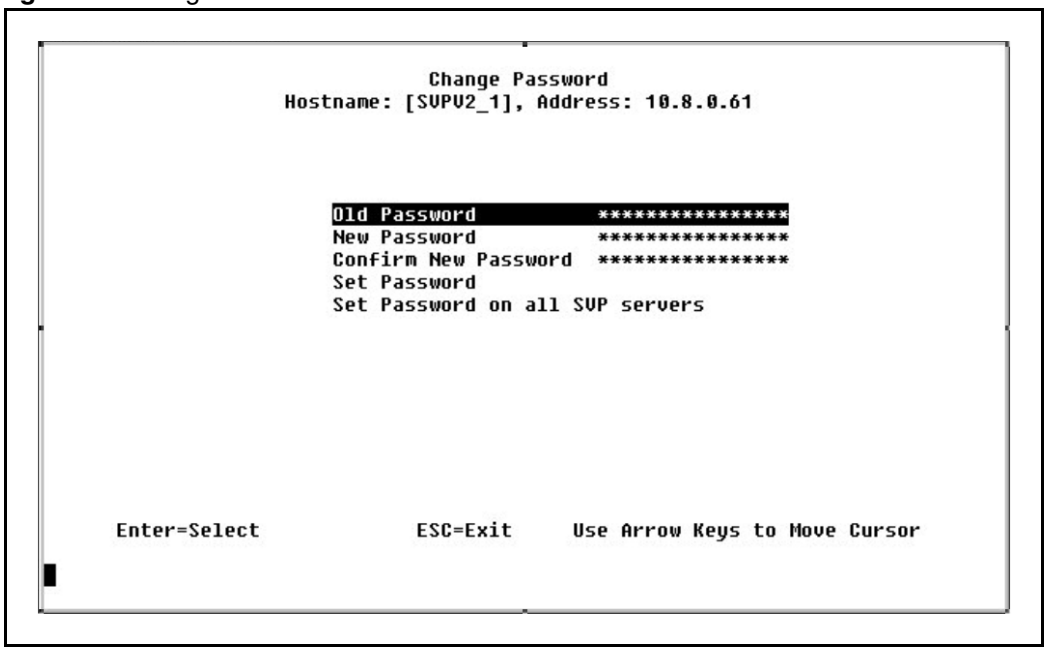
Nortel recommends that the default password be changed. Follow the steps in Procedure to change the default or existing password.

To change the password

1 Select **Change Password** from the **NetLink SVP-II System** menu.

The **Change Password** screen appears. See Figure 8.

Figure 8 Change Password screen



2 Enter the old password, enter the new password, and confirm the new password.

The password parameters are as follows:

- must be more than four characters in length
- first character must be a letter
- other characters can be a letter or a number
- dashes, spaces, and punctuation marks are not allowed (alphanumeric only)

3 Select **Set Password** and press **Enter**. Alternatively, press the **S** key on the keyboard.

IMPORTANT!

Record the password and keep it in a safe place.

If the password is forgotten, contact Nortel Technical Support for assistance.

Now it is necessary to configure the wireless handsets. See Chapter 7, "WLAN Handset configuration.

Chapter 7
WLAN Handset configuration

Wireless handset configuration is performed after the WLAN IP Telephony Manager 2245 has been installed and configured. The steps to configure a wireless handset must be performed for each wireless handset. The configuration cradle, attached to a personal computer, automates the configuration process.

System provisioning

Provision the handset on the BCM system in the same manner as an IP Phone 2004.

Configuration tasks

To enable the handsets to operate on the WLAN system, perform the following tasks:

1. Configure handset. See "Configuring the handset" on page 63 and "Configuration cradle" on page 85.
2. Program the features on the wireless handset. See "Feature programming" on page 82.
3. Test the wireless handset. See "Testing the wireless handsets" on page 94

Note: The handsets require special configuration to enable them to communicate with the optional WLAN Application Gateway 2246. Ensure that these settings are correct. See "Opening and using the Admin menu on the handset" on page 64.

The configuration cradle is an accessory to the handsets. Use the configuration cradle to create and save configuration snapshots, save the configuration from an already-programmed handset, and write a saved configuration to a handset. For more information, see "Configuration cradle" on page 85.

Configuring the handset

Configure the WLAN Handsets using:

- Configuration cradle
- Administration Menu on the handset

Configuring the handset using the configuration cradle

The configuration cradle and its software provide an automated method to configure multiple handsets. A full description is found in "Configuration cradle" on page 85.

Opening and using the Admin menu on the handset

The Admin menu contains configuration options that are stored locally on each wireless handset. Every wireless handset is independent. If the default settings are not desired, the Admin options must be configured in each separate wireless handset that requires different settings.

For a diagram of the handset, see Figure 10 on page 84.

Follow the steps in "To open and use the Admin menu on the wireless handset to open and use the Admin menu on the wireless handset.

To open and use the Admin menu on the wireless handset

1. With the wireless handset powered OFF, simultaneously press and hold the **Power On/Start Call** and **Power Off/End Call** keys.
2. Release the **Power On/Start Call** key, then release the **Power Off/End Call** key.

   The first option on the Admin menu appears.

Note: If an Admin Password has been configured, the display requires its entry before opening the Admin menu. If no password is configured, the display proceeds directly into the Admin menu.

---

3. Press the **Up**, **Down**, and **Select** side buttons, and the softkeys on the wireless handset to scroll through the menu options.

   An asterisk (*) next to an option indicates that it is selected.

   - Press the **Up/Down** buttons to display the previous/next menu items.
   - Press the **Select** button to select the menu option or item.
   - Alternatively, press the **OK** softkey to select the menu option or item.
   - Press the **Save** softkey to save the entry.
   - Press the **Bksp** key to backspace when editing the entry.
   - Press the **Up** softkey to return to the previous menu level.
   - Press **Cncl** to cancel the entry and return to the previous menu level.
   - Press the **Exit** softkey to exit the menus.

To make an alphanumeric string entry

1 On the keypad, press the **Select** button to change the entry.

2 Press the number key of the desired letter.

The number displays.

3 Press the number key again to display the first letter associated with that key.

4 Press the key again to scroll through the letters associated with that key.

Example: if **2** is pressed repeatedly, 2, A, B, C, a, b, and c are displayed.

The following table shows which keys to use to enter non-numeric characters or other characters not represented on the keypad.

To enter...	Press
. - _ ! # $ % & ‘ ( ) , : ; / \ = @ ~	1
Space	0
Q q	7
Z z	9

5 When the correct entry displays, press the right arrow to move to the next character. Repeat for each digit/letter of the entry.

6 Press the **Save** softkey to save the entry and return to the menu.

7 Press the **Exit softkey** to abort and return to the menu without saving any changes.

Admin menu options

Table 11 on page 66 lists the Admin menu items. Detailed descriptions of each item follow the table.

Note: The default settings are indicated with an asterisk (*****).

Note: In the Transmit Power section, the 50 mW and 30 mW settings only appear if the Regulatory Domain is set to None or 01.

Table 11 Admin menu options

Admin menu option	2nd level	3rd level	4th Level	5th Level
Phone Config	License Option	Set Current	[List per download]	
	Terminal Type	I2004 3rd Party		
	OIA On/Off	Enable OIA Disable OIA		
	Push-to-Talk	Allowed Channels	*Channel 1 *Channel 2 *Channel 3 *Channel 4 *Channel 5 *Channel 6 *Channel 7 *Channel 8	
		Allow/Disallow	*Allow PTT Disallow PTT	
	Admin Password	Enter PW	Re-enter Password	

Table 11 Admin menu options

Admin menu option	2nd level	3rd level	4th Level	5th Level
Network Config	IP Addresses	*Use DHCP		
		Static IP	Phone IP TFTP Server IP Default Gateway Subnet Mask Syslog Server IP SVP IP Addr	
		Svr1	Srvr 1 IP Addr Srvr 1 Port Srvr 2 IP Addr Srvr 2 Port OIA Server IP	
	ESSID	*Learn Once Learn Always Static Entry		
	Security	*None		
		WEP	Authentication	Open System Shared Key
			WEP On/Off	
			Key Information	Default Key Key Length Key 1-4
			Rotation Secret	
		Cisco FSR	Username Password	

Table 11 Admin menu options

Admin menu option	2nd level	3rd level	4th Level	5th Level
Network Config (continued)	Security (continued)	WPA-PSK	Passphrase Direct Entry	
		WPA2-PSK	Passphrase Direct Entry	
		VPN	VPN Server IP	
			VPN Client IP	Static IP IKE Mode Config
			Phase 1 – ISAKMP	Mode Authentication Diffie-Hellman Auth. Hash Encryption Local ID Lifetime (sec) Options
			Phase 2 – ESP	Auth. Hash ESP Encryption Remote Network Lifetime (sec)
	Reg. Domain: none			
Network Config (continued)	Transmit Power	*Maximum 50 mW 30 mW 20 mW 15 mW 10 mw 5 mW (See Note)		

Table 11 Admin menu options

Admin menu option	2nd level	3rd level	4th Level	5th Level
Diagnostics	Run Site Survey			
	Diagnostics Mode	Diagnostics On *Diagnostics Off		
	Syslog Mode	*Disabled Errors Events Full		
Restore Defaults				

License Option

License Option enables selection of the VoIP protocol that the site is licensed to download and run. The UNIStim Protocol to use for the handsets is **010**. Any other protocol causes the wireless handset to malfunction.

After selecting the correct protocol for the site, Nortel recommends upgrading the software for the wireless handsets.

Terminal Type

Select I2004. The Terminal type configures the wireless handset for the type of PBX in use. The BCM requires the third-party setting.

OAI On/Off

The Nortel Open Application Interface (OAI) enables the wireless handset to connect with the optional WLAN Application Gateway 2246. This device allows third-party computer applications to display alphanumeric messages on the wireless handset display and take input from the wireless handset keypad. See Appendix A, “WLAN Application Gateway 2246 for more information.

If a WLAN Application Gateway 2246 is installed in the system, OAI may be optionally enabled in each wireless handset. Select whether the wireless handset should attempt to connect to the WLAN Application Gateway 2246 by choosing either the Enable or Disable options in this menu.

If OAI is enabled, and a WLAN Application Gateway 2246 IP address is available to the wireless handset (either through DHCP or Static IP configuration), then the wireless handset communicates with the WLAN Application Gateway 2246 at power-on, and then periodically during the time the wireless handset is powered on.

Note: If a WLAN Application Gateway 2246 is not installed at the site, disable the OAI feature to preserve network bandwidth and battery life.

Push-to-talk

All eight push-to-talk channels are allowed by default. The push-to-talk menu contains the following options:

- **Allowed Channels** — toggle the status of any allowed channel, by scrolling to the channel to be disallowed and pressing the Select button. Allowed channels are displayed with a star (*) in the left column. Only the allowed channels will appear on the Standby menu, where they can be enabled or disabled by the user.
- **Allow/Disallow** — enables or disables push-to-talk. Scroll to Disallow PPT and press the **Select** button to disable push-to-talk.

  Push-to-talk is available only on the WLAN Handset 2211.

Admin Password

The optional Admin Password controls access to the administration functions in the Admin menu of the wireless handset. Configure the password in each wireless handset for which controlled access is desired. Wireless handsets are shipped without any Admin password.

Data entry for the password uses the alphanumeric string entry technique. Type the password and press the **Save** soft key. A confirmation prompt will appear. Type the password again and press the **Save** soft key. If the passwords match, the Admin password has been configured.

Note: If this option is selected on a wireless handset that already has a configured password, and the **Exit** softkey is pressed with no entry, the password is erased. This means that the wireless handset will not require an Admin password to access the Admin menu.

IMPORTANT!

Record the wireless handset Admin password and store it in a safe place. If the password is lost or forgotten, contact Nortel Technical Support.

IP Addresses menu

There are three modes in which the wireless handset can operate: DHCP-enabled, Static IP or Svr1 (Server 1). Select the mode for operation from the IP Address menu:

- *** Use DHCP —** use Dynamic Host Configuration Protocol (DHCP) to assign an IP address each time the wireless handset is turned on. If DHCP is enabled, the wireless handset also receives all other IP address configurations from DHCP.
- **Static IP —** allows a fixed IP address to be manually configured. If this option is selected, the wireless handset prompts for the IP addresses of each configurable network component. When entering IP addresses, enter the digits only, including leading zeroes. No periods are required.

- **Server1 (Srvr1)** — allows the IP addresses and ports of the primary and secondary servers and OIA server to be configured either statically or through DHCP.

Regardless of the mode in which the wireless handset is operating, the following components must be configured:

- **Phone IP** — the IP address of the wireless handset. This is automatically assigned if DHCP is used. If using Static IP configuration, obtain a unique IP address for each wireless handset from the network administrator.
- **SVP Server IP** — the IP address of the master of the WLAN IP Telephony Manager 2245 group. If using Static IP configuration, this is simply the IP address of the WLAN IP Telephony Manager 2245. The WLAN IP Telephony Manager 2245 must be statically configured to have a permanent IP address. If DHCP is being used, the wireless handset will try the following, in order: the DHCP option 151, then a DNS lookup of "SLNKSVP2" if the DHCP options 6 (DNS Server) and 15 (Domain Name) are configured.
- **Server 1 IP** — the TLAN node IP address of the LTPS IP Telephony Node on the Call Server. If the wireless handset is using static IP address configuration, enter the TLAN node IP address of the LTPS IP Telephony Node on the Call Server. If the WLAN handset is using DHCP, the DHCP server must be configured to provide the TLAN node IP address (and UDP port number) of the LTPS IP Telephony Node on the Call Server using one of the following DHCP options:
  46, 128, 144, 157, 191, and 251.
- **Server 1 Port** — the UDP port number used by the wireless handset to contact the LTPS Node Connect Service to request registration with the LTPS and the Call Server. If the wireless handset is using static IP address configuration, enter port number 7000. If the WLAN handset is using DHCP, the DHCP server must be configured to provide the TLAN node IP address and UDP port number of the LTPS IP Telephony Node on the Call Server using one of the following DHCP options:
  46, 128, 144, 157, 191, and 251.

The following components can be configured optionally:

- **TFTP Server IP** — the IP address of the TFTP Server on the network that holds software images for updating the wireless handsets. If this feature is configured (not set to 0.0.0.0 or 255.255.255.255), either through Static IP configuration, through using DHCP option 66 (TFTP Server), or the Boot server/next server (siaddr) field, the wireless handset checks for different software each time it is powered on or comes back into range of the network. This check takes only five to seven seconds and ensures that all wireless handsets in the network are kept up-to-date with the same version of software.

Note: It does not matter if the software version on the TFTP Server is newer or older; if the versions are different, the wireless handsets download the software from the TFTP Server.

- **OAI Server IP** — the IP address of the WLAN Application Gateway 2246 (if using). If using Static IP configuration, this is simply the IP address of the WLAN Application Gateway 2246. If DHCP is being used, the wireless handset tries DHCP option 152.

- **Default Gateway and Subnet Mask** — used to identify subnets when using a complex network that includes routers. Both of these fields must be configured (not set to 0.0.0.0 or 255.255.255.255) to enable the wireless handset to contact any network components on a different subnet. They can be configured using Static IP configuration or through DHCP options 3 (Default Gateway) and 1 (Subnet Mask) respectively. Contact the network administrator for the proper settings for the network.

Note: The wireless handsets cannot "roam" across subnets, since the wireless handsets cannot change their IP address while operational. Ensure that all the APs are attached to the same subnet for proper operation. The wireless handset can change subnets if DHCP is enabled, and the wireless handset is powered off, then back on, when within range of APs on the new subnet.

- **Server 2 IP** — the IP address of the secondary Nortel device. Currently, the wireless handset does not make use of this information. If using Static IP configuration, this is simply the IP address of the device. If DHCP is being used, the wireless handset tries to obtain the device's IP address and port information using the following DHCP options:
  46, 128, 144, 157, 191, and 251.
- **Server 2 Port** — the port number used by the secondary Nortel device to communicate with IP phones. Currently, the wireless handset does not make use of this information. If using Static IP configuration, consult the device documentation for port numbers. If DHCP is being used, the wireless handset tries to obtain the device's IP address and port information using the following DHCP options:
  43, 128, 144, 157, 191, and 251.
- **Syslog Server IP** — the address of the syslog server. See "Diagnostic Tools" on page 95 for more information.

ESSID

Select the option that enables the wireless handset to acquire APs with the correct ESSID (Extended Service Set ID, or Extended SSID) each time it is turned on.

With regard to Automatic Learn options, Broadcast ESSID must be enabled in the APs for ESSID learning to function (or contact the AP vendor for specifics). Overlapping wireless systems complicate the use of ESSID learning, as the wireless handset in an overlapping area could receive conflicting signals. If this is the situation at the site, use Static Entry or Learn Once in an area without overlapping ESSIDs.

- *** Learn Once** — allows the wireless handset to scan all ESSIDs for a DHCP server and/or TFTP Server. After either is found, the wireless handset retains the ESSID from whichever AP it associates with at that point. When overlapping wireless systems exist, the Learn Once feature allows the wireless handset to use only the ESSID established the first time at all subsequent power-ons. This ESSID is retained by the wireless handset until the ESSID option is reselected.

- **Learn Always** — allows the wireless handset to automatically learn the ESSID at each power-on or loss of contact with the wireless LAN (out of range). This may be useful if the wireless handset will be used at more than one site.
- **Static Entry** — if the APs do not accept broadcast ESSID, or if there are overlapping wireless systems in use at the site, enter the correct ESSID manually.

Security

The following are the security options:

- *** None** — disables any 802.11 encryption or security authentication mechanisms.
- **WEP** (Wired Equivalent Privacy) — a wireless encryption protocol that encrypts data frames on the wireless medium, providing greater security in the wireless network. If WEP Encryption is required at this site, each wireless handset must be configured to correspond with the encryption protocol set up in the APs. Select the entries from the following options to enable the wireless handset to acquire the system.

Note: By default, WEP options are off. If WEP is desired, options must be configured in the wireless handset that match those configured in the APs.

Note: Encryption codes are displayed as they are entered. For security reasons, codes are not displayed when a user returns to the Admin menu Encryption options.

Note: WEP can be set to “optional” at the AP if there are wireless devices in use that do not have WEP capability. All wireless devices must be upgraded to WEP capability for a fully secured WEP environment.

Note: WEP settings must match the AP settings.

- Set each of the following options to match exactly the settings in the APs:
  - **Authentication** — select either Open System or Shared Key.
  - **WEP** — select either WEP Off or WEP On.
  - **Key Information** — scroll through the options.
    - — **Default Key** — enter the pre-shared key number specified for use by the wireless handsets. This will be 1 through 4.
    - — **Key Length** — select either 40-bit or 128-bit depending on the key length specified for use at this site.

— **Key 1-4** — scroll to the key option that corresponds to the Default Key that was entered above. Press Select and enter the encryption key as a sequence of hexadecimal characters. Use the 2 and 3 keys to access hexadecimal digits A-F; use softkeys to advance to the next digit and backspace. For 40-bit keys, enter 10 digits; for 128-bit keys, enter 26 digits. The display scrolls as needed.

— **Rotation Secret** — used for proprietary WEP key rotation if this feature is supported in the system.

- **Cisco FSR** — to provide the highest level of security without compromising voice quality on Cisco Aironet WLAN APs, the Fast Secure Roaming (FSR) mechanism has been implemented. FSR is designed to minimize call interruptions for wireless handset users as they roam throughout a facility. Existing Aironet 350, 1100, and 1200 APs may require a firmware upgrade to support FSR. Cisco FSR requires advanced configuration of the Cisco APs in the site. See the Cisco representative for detailed documentation on configuring the APs and other required security services on the wired network. To configure Cisco FSR in the wireless handset, enter a Radius Server username and password into each wireless handset.

  — **Username** — enter a username that matches an entry on the Radius server. Usernames are alphanumeric strings, and can be entered using the alphanumeric string entry technique.

  — **Password** — enter the password that corresponds to this Username.

- **WPA-PSK** — Wi-Fi Protected Access (WPA) using Pre-Shared Key (PSK) provides enhanced security and can be used, if supported by the APs. Select one of the following options:

  — **Passphrase** — enter a passphrase. The passphrase can be from 1 to 63 ASCII characters or 64 hexadecimal digits. Do not choose a simple word because password-cracking programs can easily extract the key and gain illicit access to the system. See “Choosing a passphrase” on page 76 for further information.

  — Example: why2fear4WPA-is-DEPLOYED_HERE

  — **Direct Entry** — enter a pre-shared key code (hexadecimal number).

Note: Consult the Configuration Note for the installed APs, at http://www.spectralink.com/service/manuals_config.html, for information on whether WPA-PSK is recommended for the AP. Configure the recommended version on the AP and configure the corresponding option on the Admin menu.

Note: WPA-PSK settings must match the AP settings.

- **WPA2-PSK** — WPA2 with PSK provides enhanced security over WPA-PSK and can be used, if supported by the APs. Select one of the following options:
  - **Passphrase** — enter a passphrase. The passphrase can be from 1 to 63 ASCII characters or 64 hexadecimal digits. Do not choose a simple word because password-cracking programs can easily extract the key and gain illict access to the system. See "Choosing a passphrase" on page 76 for further information.
    - Example: why2fear4WPA2-is-DEPLOYED_HERE
  - **Direct Entry** — enter a pre-shared key code (hexadecimal number).

Note: Consult the Configuration Note for the installed APs, at http://www.spectralink.com/service/manuals_config.html, for information on whether WPA-PSK is recommended for the AP. Configure the recommended version on the AP and configure the corresponding option on the Admin menu.

Note: WPA-PSK settings must match the AP settings.

- **VPN** — selecting VPN for security requires that a secure tunnel be established for the transfer of information. The data itself no longer needs to be encrypted because the VPN tunnel is already encrypted. VPN security requires a number of configuration steps, and is easily configured using the Configuration Cradle (see "Configuration cradle" on page 85 for more information). VPN security is also closely tied with the VPN server configuration. Only the WLAN Handset 2212 supports VPN security.

Note: The VPN server must support the handset configuration.

  - **VPN Server IP** — the IP address of the VPN server on the public (unsecure) side of the network.
  - **VPN Client IP** — the IP address that appears to be part of the private (or secure) network
    - **Static IP** — the address can be statically programmed in the handset, in which case it must match the address assigned to the handset in the VPN server.
    - **IKE Mode Config** — if the VPN server supports the ISAKMP Mode Configuration, it can assign the IP address automatically.
  - **Phase 1 – ISAKMP** — this is the first phase of the tunnel negotiation process. It establishes a set of security parameters (the ISAKMP Security Association) that will be used to encrypt the negotiation of the actual tunnel parameters in Phase 2. In essence, Phase 1 protects Phase 2.
    - **Mode** — VPNs can negotiate their parameters using two different modes. These are called Main Mode and Aggressive Mode. Aggressive Mode is the most flexible of the two\ and is the only one currently supported by the handsets.
    - **Authentication** — enter a pre-shared key, which must match the shared secret key entered for the handset in the VPN server. The key may be an ASCII string or a hexadecimal string.

- **Diffie-Hellman** — choose **Group 1**, **Group 2** or **Group 5**, depending on the level of security required and the level supported by the VPN server.
- **Auth. Hash** — choose either **MD5** or **SHA**, depending on the VPN server setting.
- **Encryption** — chooses **DES** or **3DES**, depending on the VPN server setting.
- **Local ID** — identifies the VPN user who is trying to connect to the server. The Local ID must match the VPN server setting.
- **Lifetime (sec)** — gives the lifetime, in seconds, of the ISAKMP security association. When the lifetime expires, the tunnel must be closed and a new one created. Nortel recommends a minimum of 12 to 24 hours (43 200 to 86 400 seconds). The maximum value for the lifetime setting is 31 days (2 778 400 seconds).
- **Options** — each of the options can be enabled individually.
  Init Contact — by enabling this option, the handset will send an initial contact request message to notify the VPN server that the handset has relinquished the old tunnel and wants to open a new one.
- **Nortel features** — enabling this option will make the handset use Nortel-specific extensions to the standard IKE negotiation. The handset will advertise itself as a Contivity-compatible client and hash the Key ID before passing the information to the Contivity.

— **Phase 2 – ESP** — this is the second phase of the tunnel, and is encrypted by the parameters established in Phase 1. Phase 2 negotiates the parameters used by Encapsulated Security Payload (ESP) to encrypt the actual traffic in the tunnel.

- **Auth. Hash** — choose either MD5 or SHA1 to match the settings in the VPN server.
- **ESP Encryption** — select DES or 3DES for the encryption algorithm for the tunnel traffic.
- **Remote Network** — enter an IP address and a network mask to specify the private (secure) network address range.
- **Lifetime (sec)** — configure a lifetime in seconds for ESP security associations. Typically, this setting is a few hours and must be no greater than the Phase 2 lifetime configured in the VPN server.

Choosing a passphrase

The choice of a good passphrase is very important to ensure the privacy of the handset data and messages. A passphrase should be:

- Known only to the administrator.
- Long enough so that it is difficult to guess or crack. For example, search programs often contain dictionary words and famous phrases.
- Difficult to guess by intuition — even by someone who knows the administrator well. Birth dates, for example, are a poor choice.
- Easy for the administrator to remember and type. Nortel does not recommend writing the password down.

Reg. (Regulatory) Domain

The Regulatory Domain defaults to None on the wireless handset display. FCC requirements dictate that the menu for changing the domain be available by password, which in this case is the LINE button. To change the domain, press LINE and then enter the digits that represent the site's domain. Both digits must be entered.

The following are domain digits:

- **01** — North America
- **02** — Europe (except Spain and France) and Japan
- **04** — Spain
- **05** — France

Note: As of this writing, Spain and France are adopting the general European Regulatory rules. Check with the wireless LAN administrator or supplier for the correct domain to enter in these countries.

Transmit Power

The Transmit Power selected must match the installed APs and all Wireless Handsets and is regulated by the domain. The maximum for North America is 100 mW, while other domains have a maximum of 30 mW. The following power settings are available:

- Maximum (default)
- 50 mW (only available in the North American domain)
- 30 mW (only available in the North American domain)
- 20 mW
- 15 mW
- 10 mW
- 5 mW

Note: If the default is not used, ensure that the Transmit Power setting is the same for all handsets and all APs.

Run Site Survey

Run Site Survey is used to check the signal strength from APs. When Run Site Survey is selected, the wireless handset remains in this mode until it is powered off. During configuration, press the right arrow to skip this mode. See "Site survey" on page 25 for more information on using this mode. See "Run Site Survey" on page 95 for a detailed description of the survey results.

Diagnostics Mode

When Diagnostics Mode is chosen from the menu, the handset enters the Diagnostics function immediately. See "Diagnostics Mode" on page 96 for more information.

Syslog Mode

Syslog Mode can be enabled or disabled. See "Syslog Mode" on page 100 for more information.

Syslog Mode is configured to one of the following:

- * Disabled — turns syslog off.
- Errors — causes the handset to only log events that are considered errors.
- Events — logs all errors, plus some events of interest.
- Full — logs all errors and all other events of interest.

Table 12 lists the syslog messages and which level of logging will produce them.

Table 12 Syslog message levels

Message Type	Errors	Events	Full
Failed Handoff	Yes	Yes	Yes
Successful Handoff	No	Yes	Yes
Security Error	Yes	Yes	Yes
Call Start/End	No	Yes	Yes
Audio error threshold exceeded	Yes	Yes	Yes
Audio stats	No	No	Yes (every 5 secs)
Radio error threshold exceeded	Yes	Yes	Yes
Radio stats	No	No	Yes (every 5 secs)

Restore Defaults

The Restore Defaults option resets all user and administrative parameters (other than License Options) to their factory defaults. During configuration, press the right arrow to skip this mode.

Downloading the wireless handset software

All handsets are shipped with a generic software load that allows them to associate to a wireless LAN and download their functional software from a TFTP Server. The wireless handsets do not function properly without downloading their appropriate software.

Pre-download checklist

The following requirements must be met to download software by over-the-air file transfer:

- A wireless LAN must be properly configured and operational through the use of 802.11a/b/g SVP-compliant wireless APs.
- The Nortel WLAN IP Telephony system must be connected to the network and completely operational.
- A TFTP Server must be available on the network in order to load the appropriate software into the wireless handsets.
- The battery pack on the wireless handsets must be fully charged.

Downloading the software

Before attempting to download the wireless handset software, ensure the following conditions have been met:

- A wireless LAN is properly configured and operational through the use of 802.11a/b/g wireless APs.
- The supported IP Telephony system is connected to the network and completely operational.
- A TFTP Server is available on the network to load the appropriate software into the wireless handsets.
- The battery pack on the wireless handset is fully charged.

To download the wireless handset software

1. Download the latest handset software from the Nortel web site.
2. Load the latest version of the handset UNIStim code software and place it on the TFTP Server. Ensure the TFTP Server is started.

   The five files that are needed are:

   - slnk_cfg.cfg
   - pd11gl3.bin
   - pd11usd.bin
   - pd11usd3.bin
   - pi110001.bin

3. If statically assigning IP addresses, ensure that the wireless handset IP address, TFTP Server IP address, Subnet Mask, and Default Gateway information are accurate in the wireless handset's Admin menu. If using a DHCP Server, ensure that the DHCP options are configured.
4. Ensure the wireless handset has properly configured ESSID and Reg Domain Information within the Admin menu. If broadcast ESSIDs are accepted at the APs, the handset automatically learns the ESSID information when powering on.
5. Using the Admin menu on the wireless handset, ensure the License Management menu option is set to 010. This ensures the handset will check for the proper UNIStim software files each time it powers on.
6. Power on the wireless handset.

   The software now downloads to the wireless handset. The status bar increments fully across the wireless handset display for each function that is being performed in the download process.
7. Upon completion of the update process, the wireless handset re-boots with the new firmware.
   a. Register the wireless handset with the BCM system as if it were an IP Phone 2004.
   b. Properly label the wireless handset with the appropriate extension number.

For future software upgrades, simply update the software files that are stored on the TFTP Server. Each time the wireless handset is powered on, it will check with the TFTP Server to ensure it has the proper software version, and download the new software if necessary.

IP Phone 2004 mapping

This section describes the mapping between the emulated IP Phone 2004 and the handsets.

Voice Messaging Access

Voicemail access is obtained through the Inbox key. Voicemail is accessed on the wireless handset as FCN + a digit that corresponds to the assigned key.

Codecs

The handsets are compatible with the G.711 and G.729A/AB codecs. No configuration is required on the wireless handsets.

DHCP

Dynamic Host Configuration Protocol is a standardized protocol that enables clients to be dynamically assigned with various configuration parameters, such as an IP address, Subnet Mask, Default Gateway, and other critical network configuration information. DHCP servers centrally manage such configuration data, and are configured by network administrators with settings that are appropriate for a given network environment.

The wireless handset searches for server configuration in the options listed in Table 13. The wireless handset will use the DHCP options listed if DHCP use is enabled.

Table 13 DHCP options

Option	Meaning
1	Subnet Mask
3	Default Gateway
6	DNS Server
15	Domain Name
43	Vendor specific*
66	TFTP Server
128	Site specific *
144	Site specific *
151	WLAN IP Telephony Manager 2245
152	WLAN Application Gateway 2246
157	Site specific *
191	Site specific *
251	Site specific *
siaddr	Boot server or next server
* Could be used to find the CS 1000/Meridian 1 device.	

TFTP

The handsets use TFTP to update the wireless handset software over the 802.11a/b/g wireless LAN.

DNS

Domain Name System (DNS), an industry-standard protocol, locates computers on an IP-based network. IP networks rely on number-based addresses to move information on the network. However, it is easier to remember names than number-based addresses. DNS translates user-friendly names into IP addresses that the network can recognize. The wireless handsets can use DNS to automatically translate names into IP addresses for the TFTP Server and the WLAN IP Telephony Manager 2245.

Feature programming

The handsets emulate the IP Phone 2004. All IP Phone 2004 functions and messaging features are supported where possible. Functions that require use of the volume keys and the Speakerphone function are not supported.

The large screen area of the IP Phone 2004 and its numerous keys are mapped onto the smaller screen and fewer buttons of the wireless handsets. The button mapping from the IP Phone 2004 to the handsets was designed to preserve nearly all of the functionality of the IP Phone 2004 within a small, mobile device.

Feature and key assignment

The line keys, numbered 1, 2, 3, 4, 5, and 6, to the left and right of the display screen of the IP Phone 2004 (see Figure 9 on page 83) are mapped to the LINE button on the handsets (see Figure 10 on page 84).

The IP Phone 2004 has several fixed feature keys. The handsets support the six features that are suitable to a mobile user through the Function (FCN) key on the wireless handset. When FCN is pressed, a screen that lists the features and the assigned keys displays. Press FCN again to display a second screen that lists more features and their assigned keys.

If a third-party application has been assigned to a key, that information appears on the Feature list. See Table 14 for fixed feature keys supported by the handsets. Keys not indicated are not supported.

Table 14 Supported fixed feature keys

Screen	Fixed feature key
First screen	1 Mute
	2 Hold
	3 Goodbye
	4 Directory
Second screen	5 Inbox
	6 Outbox
	7 Optional third-party application
	8 Optional third-party application
	9 Optional third-party application

If an OAI application is operational, a function key sequence is assigned in the OAI application's configuration and overrides any function sequence established here. Therefore, FCN+7, FCN+8, or FCN+9 is a good choice for the OAI sequence.

Figure 9 IP Phone 2004

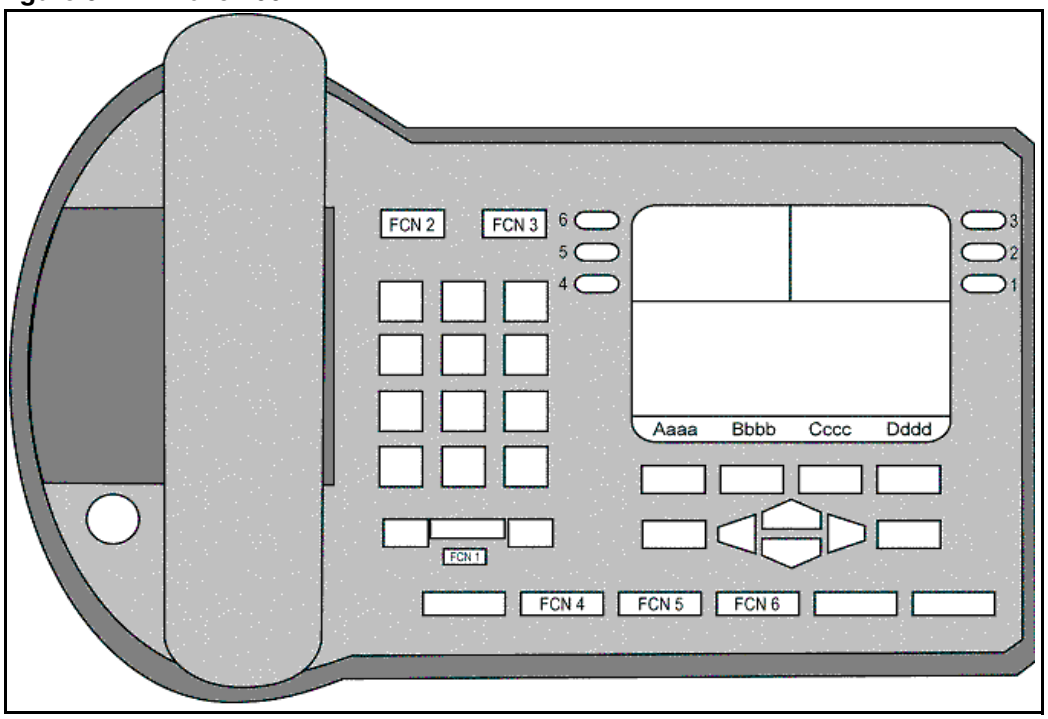


Figure 10 WLAN Handset 2210

Note: The WLAN Handset 2210, WLAN Handset 2211, and WLAN Handset 2212 have the same button and screen layout.

Table 15 lists how the keys of the IP Phone 2004 are mapped to key sequences on the wireless handsets.

Table 15 IP Phone 2004 mapping to the wireless handsets

IP Phone 2004 key	Feature	Wireless handset key sequence
1	Programmable	Line + 1
2	Programmable	Line + 2
3	Programmable	Line + 3
4	Programmable	Line + 4
5	Programmable	Line + 5
6	Programmable	Line + 6
Mute	Mute	Fcn + 1
Hold	Hold	Fcn + 2

Table 15 IP Phone 2004 mapping to the wireless handsets

IP Phone 2004 key	Feature	Wireless handset key sequence
Goodbye	Goodbye	Fcn + 3
Directory	Directory	Fcn + 4
Inbox	Inbox	Fcn + 5
Outbox	Outbox	Fcn + 6
Softkey	Programmable	Softkey A
Softkey	Programmable	Softkey B
Softkey	Programmable	Softkey C
Softkey	Programmable	Softkey D

Program keys on the wireless handset

The Line keys 1-6 on the handsets are programmable by the end user. These Line keys can be programmed in the wireless handset in the same manner they are programmed on the IP Phone 2004.

To program the keys on the wireless handset

1. Place the wireless handset in the idle state by pressing **Power On/Start Call**.
2. Press **FCN + 3**.

   The wireless handset is in the Active (idle) state. The softkey display area is active but there is no dial tone.
3. Select the Line key to be programmed.
4. Enter the number and save the entry.

For information on using the wireless handset features, refer to the *WLAN Handset 2210/2211/ 2212 User Guide*.

Configuration cradle

The configuration cradle is an optional accessory. It is designed to automate the configuration of the wireless handsets.

The cradle is connected to a personal computer (PC) through one of the communication (COMM) ports. Software for the PC is downloaded from the Internet. The software is installed on the PC and configured to read from the COMM port.

Note: Use of adapters or port replicators is not recommended, since they do not properly handle the communications between the cradle and the PC.

Personal Computer Requirements

The software runs on Windows NT/2000/XP.

Note: Use only the supplied power adapter.

Note: Do not immerse the cradle in water or other liquids. Do not pour liquids into the slots.

Note: Do not place anything in the cradle other than the WLAN Handset 2210, WLAN Handset 2211 or WLAN Handset 2212, or damage the contacts. Damaged contacts will not allow the cradle to work correctly.

Note: The operating environment should be 10° to 30° C (50° to 85° F). Do not expose the cradle to freezing temperatures or direct sunlight.

Note: Only one handset can be configured at a time.

Configuration cradle safety notes

- The configuration cradle operates in a 50 to 85 degrees F (10 to 30 degrees C) environment. Do not expose to freezing temperatures or sunlight.
- Use only the original Nortel plug-in power adapter.
- Place only one phone in the cradle at a time.
- Do not place a phone in the cradle with a battery installed.
- Do not immerse the cradle in water or other liquid.
- Do not pour liquids into the telephone slots.
- Only use Nortel telephones in this cradle.

To install and configure the configuration cradle

1. On the PC, create a folder for the software.
2. Using a web browser:
   - **a** Connect to http://www.spectralink.com/service/software.php
   - **b** Locate the entry for the NetLink Configuration Cradle.
   - **c** Click the product link and save the “Configuration Cradle.exe” file to the folder created in step 1.
   - **d** (Optional) Copy the release notes to the folder created in step 1.

3 Double-click on the “Configuration Cradle.exe” file to install the software, putting the files into the folder created in step 1.

4 The tool does not require any additional installation and does not show up in the Programs menu or in the computer Registry.

5 (Optional) To aid in locating the tool quickly, create a shortcut on the computer desktop to the PhoneConfig.exe file.

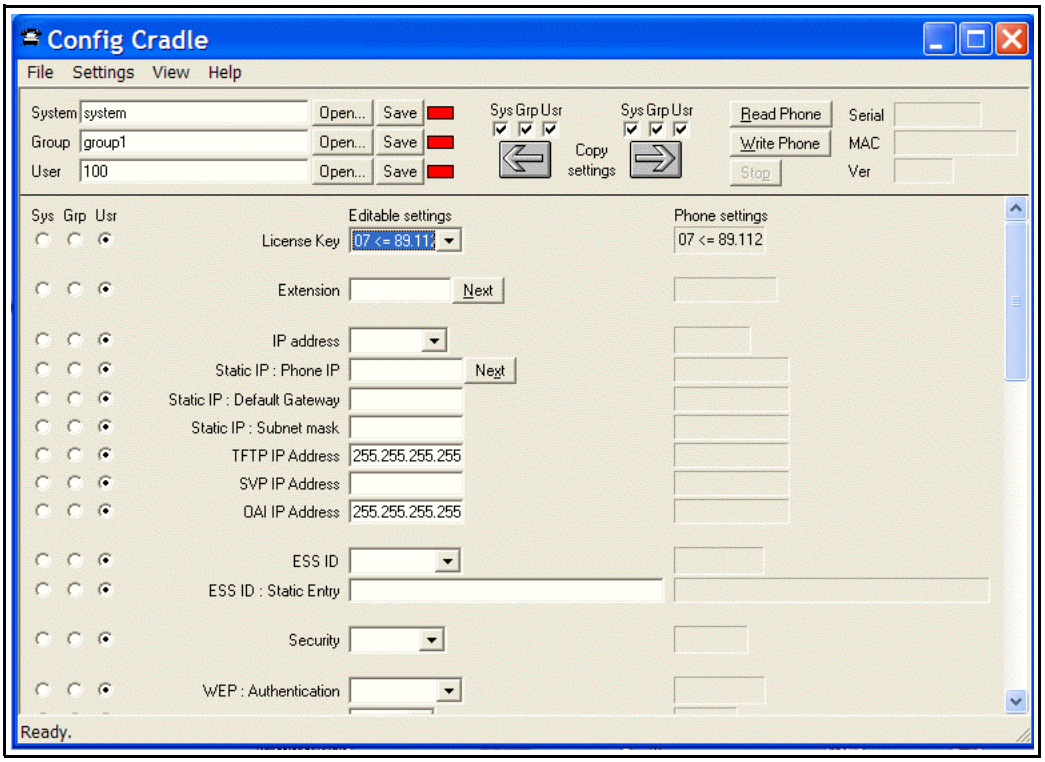
6 Place the cradle on a flat horizontal surface and plug the power supply into the cradle and into an appropriate power outlet.

7 Connect the cradle, using a serial cable with a DB-9 connector, to one of the COMM ports of the PC.

8 Double-click on the PhoneConfig.exe file or the shortcut created in step 5.

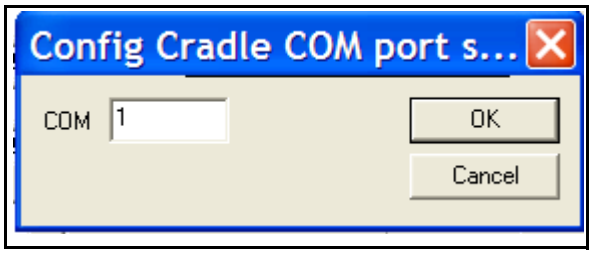
The **Config Cradle** screen opens, as shown in Figure 11.

Figure 11 Config Cradle screen



9 From the menu at the top of the screen, select **Settings > COM port** and enter the port number of the COMM port that the cradle is using (see Figure 12 on page 88).

Figure 12 COM port screen



10 Click **OK**.

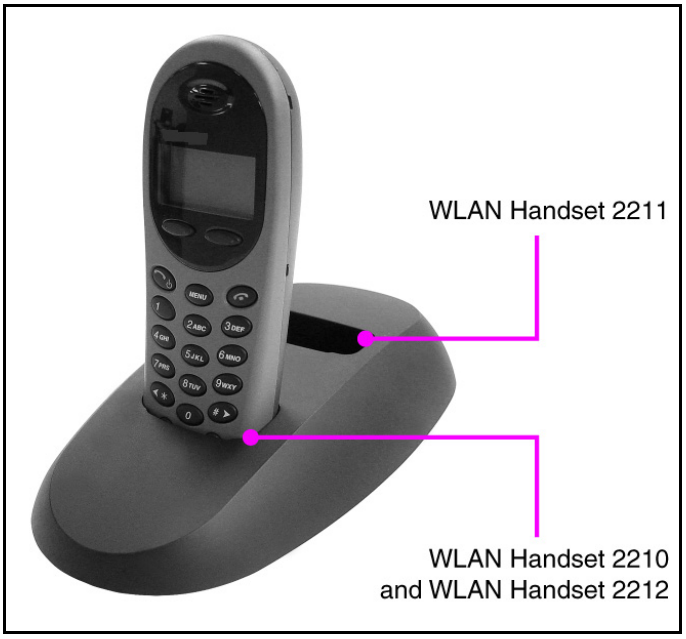
11 The software is now installed and configured.

Note: If software updates are required, overwrite the installed files with the new files. The existing configuration files will be retained.

Using the configuration cradle and software

The cradle contains two slots, one for the WLAN Handset 2210 and WLAN Handset 2212 and the other for the WLAN Handset 2211 (see Figure 13). When a handset is placed in the appropriate slot in the cradle, its configuration can be read using the software, and stored as a file on the personal computer. Handset profiles that are saved on the PC can be downloaded to the handset. Profiles can also be created independent of the handset.

Figure 13 Configuration cradle



A series of master configuration files can be planned and created using the software. See "Planning the configuration files" on page 89 for a description of files. Planning should be done before any handsets are configured.

After the planning is complete, use the following procedures to:

- Read and save a handset configuration — see "Reading and saving a handset configuration" on page 91.
- Create a new master configuration file — see "To create a new master configuration file" on page 93.
- Create a new configuration file using the master files — see "To create a new configuration using the master files" on page 93.
- Change an existing configuration file — see "To change an existing configuration file" on page 93.
- Change a configuration from a handset — see "To change a configuration obtained from a handset" on page 94
- Download a configuration to a handset — see "To download a configuration to a handset" on page 94.

Planning the configuration files

Careful planning of the configuration files reduces the number of custom changes that have to be done on the individual handsets. The software for the configuration cradle allows any number of files to be saved.

Settings can be categorized into four types:

- **System** (**Sys**) — options that are stable across the system. Typically, these include:
  - License Option
  - Network Config
  - IP Addressing
  - ESSID
  - Security
- **Group** (**Grp**) — options that are common to groups of users. Typically, these include:
  - Push to Talk Allow/Disallow
  - Push to Talk Channel
  - Zones
- **User** (**Usr**) — options that are default values or may be changed later by the user. Typically, these include:
  - Ring Options
  - Phone Options
- Custom user options — options that vary on an individual handset basis. Typically, these include:
  - Static IP Address
  - Extension

Use the available options listed in "Admin menu options" on page 66 to determine which options belong in each master category (Sys, Grp or Usr). Each option should be in only one category. Custom user options do not require any additional planning.

After the different categories are determined, each category should have a separate copy of the worksheet, located in "Configuration cradle worksheet" on page 108. Assign a different descriptive file name to each worksheet.

Once the category worksheets are created, use "To create a new master configuration file" on page 93 to create each of the required master configuration files. Create the master files in the following order:

1. System options
2. Group options
3. User options

Finally, when the planning and master files are completed, use the "To create a new configuration using the master files" on page 93 to create the profile for each individual handset and use the cradle to download the profile to the handset.

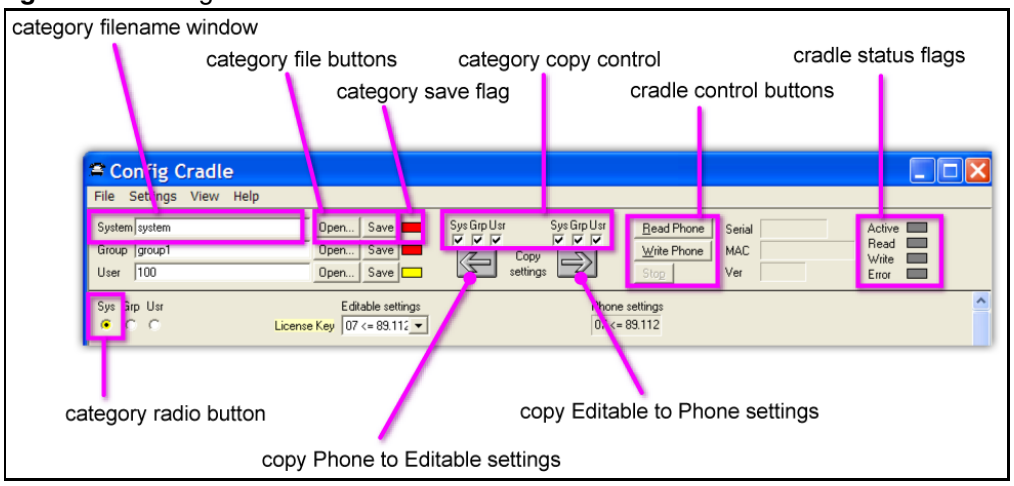
Configuration cradle software

The software allows you to:

- name, open and save configuration files
- download and upload configuration settings to and from the handset in the cradle.
- configure options in the Sys, Grp and Usr categories.

The top of the screen is shown in Figure 14.

Figure 14 Configuration cradle software toolbar



The top portion of the screen is the toolbar, and the bottom portion is the configuration area. Only part of the configuration area is shown in Figure 14.

On the left side of the screen is the category file control area. Each category (System, Group and User) has a filename window, file buttons (Open… and Save) and a save flag. Each save flag displays different colors, depending on the status of the file:

- Red — file does not exist. The filename in the window has not been created.
- Yellow — file not loaded. The filename in the window exists, but has not been loaded into the Editable settings column.
- Green — unsaved edits. Changes have been made in the Editable settings column, but not written to the file.
- Gray — file up to date. The settings have been saved.

To the right of the category file control area is the copy control area, made up of the category copy control boxes and the arrow buttons. The left arrow is used to copy the information in the Phone settings column to the Editable settings column. The right arrow is used to copy the information from the Editable settings column to the Phone settings column. The check boxes above these arrows control which categories are copied.

Next to the copy control area is the cradle control area, made up of the control buttons, flags and information area. The cradle control buttons (Read Phone, Write Phone and Stop) control the communication between the software and the cradle. If no handset is in the cradle when the buttons are pressed, an error message is displayed. When the handset is read, its information (Serial number, MAC address and software version) are displayed in the boxes. The status flags display the action in progress with the cradle (Active, Read, Write, Error).

Below the toolbar is the configuration area. Each configurable option is displayed, with a set of category radio buttons. The category radio buttons are used to indicate which category the option has been assigned to. An option can exist in only one category. The option box in the Editable settings column is where changes can be made. The option box in the Phone settings column is read-only.

Note: When entering security keys, the cradle displays the key as entered. This is different from the way the handset handles the display through the Admin menu (key is not displayed).

Reading and saving a handset configuration

Follow the steps in the procedure to read and save the configuration of an already-configured handset. The configuration cradle must have been previously installed using see “To install and configure the configuration cradle”.

To read and save the configuration of an existing handset

1 Start the **Config Cradle** software by double-clicking on the PhoneConfig.exe file of the tool. The tool appears, as shown in Figure 11 on page 87.

2 Remove the battery from the handset.

3 Place the handset in the proper slot in the cradle (see Figure 13 on page 88).

4 Press the **Read Phone** softkey in the **Config Cradle** screen.

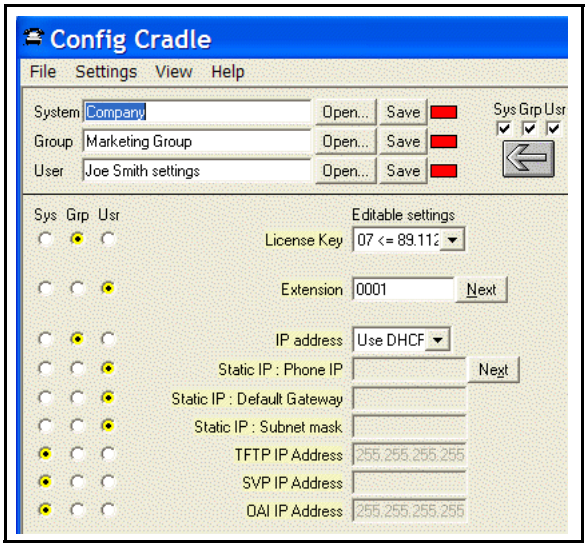
The configuration of the phone is read and appears in the right hand column, labeled **Phone settings**.

5 Press the button. The configuration data is copied from the **Phone settings** column to the **Editable settings** column.

6 (Optional) Press the radio button associated with each item to designate which category (**Sys**, **Grp**, **Usr**) the item belongs in.

7 Enter a file name in the name box beside the category. The items which belong in the category are highlighted in yellow (see Figure 15 and explanation in Table 16 on page 92).

Figure 15 File naming example



The Table 16 describes the files being created, as shown in Figure 15 on page 92.

Table 16 File name description

File name	Description
Company	System-wide settings
Marketing Group	Settings for the Marketing Group
Joe Smith settings	Joe Smith's unique settings

8 Press the **Save** button for the appropriate category to save the settings. The red box beside the **Save** button will change to green when the save is complete.

To create a new master configuration file

1 Start the **Config Cradle** software by double-clicking on the PhoneConfig.exe file of the tool. The tool appears, as shown in Figure 11 on page 87.

2 Using the worksheet, enter the options for the category and press the appropriate category radio button.

3 When all the options are entered, change the name beside the file buttons to match the name entered in the worksheet.

For example, if the options were for a group, enter “Marketing Group” in the box beside **Group**.

4 Press the **Save** button associated with the category.

5 The configuration is saved to the named file.

To create a new configuration using the master files

1 Start the **Config Cradle** software by double-clicking on the PhoneConfig.exe file of the tool.

The tool appears, as shown in Figure 11 on page 87.

2 Press the **Open** button for the System options and select the name of the master system file.

3 Press the **Open** button for the Group options and select the name of the master group file.

4 Press the **Open** button for the User options and select the name of the master user file.

5 Set any custom user options.

6 Enter a name in the User box and press the associated **Save** button.

7 (Optional) To download the configuration to a handset see “To download the wireless handset software”.

To change an existing configuration file

1 Start the **Config Cradle** software by double-clicking on the PhoneConfig.exe file of the tool. The tool appears, as shown in Figure 11 on page 87.

2 Press the **Open…** button associated with the category required and select the name of the file to be opened.

3 The file is read and the settings appear in the **Editable settings** column.

4 Make the changes necessary.

5 Press the **Save** button to update the configuration file.

To change a configuration obtained from a handset

1. Start the **Config Cradle** software by double-clicking on the PhoneConfig.exe file of the tool. The tool appears, as shown in Figure 11 on page 87.
2. Remove the battery from the handset.
3. Place the handset in the proper slot in the cradle (see Figure 13 on page 88).
4. Press the **Read Phone** softkey in the **Config Cradle** screen.

   The configuration of the phone is read and appears in the right hand column, labeled **Phone settings**.
5. Press the button. The configuration data is copied from the **Phone settings** column to the **Editable settings** column.
6. Change the data as required.
7. (Optional) Save the configuration to a file.
8. (Optional) To download the configuration to a handset, go to "To create a new master configuration file" on page 93.

To download a configuration to a handset

1. Start the **Config Cradle** software by double-clicking on the PhoneConfig.exe file of the tool. The tool appears, as shown in Figure 11 on page 87.
2. Open the files required for the handset.
3. Remove the battery from the handset.
4. Place the handset in the proper slot in the cradle (see Figure 13 on page 88).
5. Press the button. The configuration data is copied from the Editable settings column to the Phone settings column.
6. Press the **Write Phone** button.
7. When complete, remove the handset from the cradle, replace the battery and test the handset configuration (see "To test the wireless handsets").

Testing the wireless handsets

Verify proper registration and operation of each wireless handset by performing the following tests on each wireless handset in an active wireless area.To test the wireless handsets see "To test the wireless handsets".

To test the wireless handsets

1. Power on the wireless handset by pressing **Power On/Start Call**. A series of messages display as the wireless handset acquires the system. The wireless handset displays the user extension or display dashes if no extension is programmed. Any error messages clear.
2. Press the **Power On/Start Call** key. The extension number is replaced by information from the Call Server and dial tone is heard. Place a call and listen to the audio quality. End the call by pressing the **Power Off/End Call** key.
3. Place a call to the wireless handset and verify ring, answer, clear transmit, and clear receive audio.
4. Use the **FCN** key to verify all programmed features on the wireless handset.
5. Press the **Power On/Start Call** key. Any line indicators turn off and the extension number display returns.

Diagnostic Tools

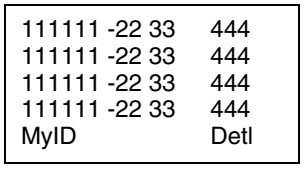
Run Site Survey, Diagnostics Mode and Syslog Mode are provided to assist the WLAN administrator to evaluate the functioning of the handset and the VoWLAN system. These tools are enabled from the handset Admin menu.

Run Site Survey

Site Survey is used to evaluate the facility coverage before certifying that an installation is complete. It can also be used at any time to evaluate coverage by testing signal strength, to gain information about an AP, and to scan an area to look for all APs regardless of ESSID. The information available through Site Survey includes:

- ESSID
- beacon interval
- information regarding support of various protocols and standards, as required
- current security configuration

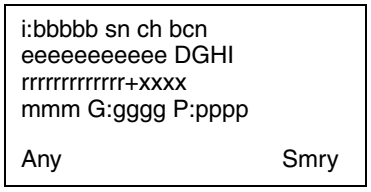
When Run Site Survey begins, it is in single ESSID mode. Press the Any soft key to switch to all APs (regardless of ESSID) mode; the Any soft key changes to MyID. The display looks like the following in multiple AP mode:



Where:

111111 = last three octets of the ESSID for the discovered AP
22 = signal strength of the specified AP
33 = channel number of the specified AP
4444 = DTIM interval configured for the specified AP
MyID = soft key to toggle between single and any ESSID mode
Detl = soft key to toggle between summary and detail screens

Press the **Detl** soft key to view the details, as follows:



Where:

i = index of selected AP (range: 0-3)
bbbbb = last three octets of the ESSID for a discovered AP
sn = signal strength in -dbm
ch = channel
bcn = beacon interval
eeeeeeeeeee = ESSID (up to first 11 characters)
DGHI = standards supported
rrrrr = rates supported (example: 1b2b5b11b)
+ = more rates supported than displayed
xxxx = WMM or UPSD if supported
mmmm = security mode
G:gggg = group key security
P:pppp = pair-wise key security
Any = soft key to toggle between single and multiple ESSID mode
Smry = soft key to return to summary display

Diagnostics Mode

Diagnostics Mode evaluates the overall quality of the link between the handsets, AP and the infrastructure equipment (call server, WLAN IP Telephony Manager 2245, and gateways). Diagnostics Mode can be used when the handset is active.

When Diagnostics Mode is activated in the Admin menu, the handset enters the diagnostic state. The handset can display diagnostics any time it is on a call.

Pressing the Menu key displays a number of diagnostic counters. Five screens of counters may be displayed by pressing the Menu key to scroll through the following screens:

- Screen 1 — displays counters for missed receive packets, missed transmit packets, receive retry count and transmit retry count.
- Screen 2 — displays jitter delta, last successful transmit data rate and gateway type.
- Screen 3 — displays a list of APs and some of their details.
- Screen 4 — displays association and re-association counts.
- Screen 5 — displays security error count and sequence number for last security error.

After all the counters are displayed, the screen returns to the normal off-hook display.

The screen number is displayed on the top line of the screen.

Screen 1

Diagnostics screen 1 displays the following:

MissedRcvCnt	nnnnn
MissedXmtCnt	nnnnn
RxRetryCount	nnnnn
TxRetryCount	nnnnn

Where:

MissedRcvCnt is the missed receive packet count since power up.
MissedXmtCnt is the missed transmit packet count since power up.
RxRetryCount is the receive retry count since power up.
TxRetryCount is the transmit retry count since power up.

Screen 2

Diagnostics screen 2 displays the following:

Jitter	nnnnn
LastRate	nnnnn
GatewayType	mnemo

Where:

Jitter is the current delta from the desired jitter buffer depth, in microseconds.

LastRate is the last successful transmit data rate.

GatewayType is a mnemonic that indicates the gateway type. The mnemonic is one of:

SAWA2	all phones are rate limited to 2 Mb because an old 2 Mb handset is on the network.
2Mb	old style 2 Mb
11Mb	New style 11 Mb

Screen 3

Diagnostics screen 3 displays a list of the APs that are heard, in the following format:

C : mmmm ch - ss	aid
1 : mmmm ch - ss	mnem
2 : mmmm ch - ss	mnem
3 : mmmm ch - ss	mnem

Where:

C is the AP currently in use.

1, 2, and 3 are the candidate APs.

mmmm is the hexadecimal number comprised of the last two octets of the AP MAC address.

ch is the channel number that the AP is configured on.

ss is the signal strength for the AP in dBm.

aid is the Association ID of the currently associated AP.

mnem is a mnemonic that indicates why the handset did not hand off to this candidate:

Unkn	reason unknown
Weak	signal strength too weak
Rate	One or more basic rates not supported
Full	AP cannot handle bandwidth requirements

AthT	Authentication Timeout
AthF	Authentication Failure
AscT	Association Timeout
AscF	Association Failure
SecT	Security Timeout
SecF	Security Failure
Cnfg	Configuration error — AP is not configured correctly (check security, QoS mode or network infrastructure)

Screen 4

Diagnostics screen 4 displays the following:

```
AssocCount      nnnnn
ReAssocCount    nnnnn
AsssocFailure   nnnnn
ReAssocFail     nnnnn
```

Where:

AssocCount is the association count since power up.

ReAssocCount is the re-association count since power up.

AssocFailure is the number of association failures since power up.

ReAssocFail is the number of re-association failures since power up.

Screen 5

Diagnostics screen 5 displays the following:

```
Sec-ErrCount    nnnnn
LstSecErrSeq    nnnnn
```

Where:

Sec-ErrCount is the security error count since power up.

LstSecErrSeq is the MAC frame sequence number with the last security error.

Syslog Mode

A syslog server must be present on the network so that the handset can send log messages and have them saved. The syslog server IP address can be configured using DHCP or statically configured.

Note: If the syslog server address is blank (000.000.000.000 or 255.255.255.255) or the handset is using DHCP and no option 7 is received from the DHCP server, the handset will not send any syslog messages.

Each syslog message includes the following:

- Date and time (to 1/100th of a second) since the handset power on (configured to January 1 00:0:00); requires an SNTP server
- WLAN Handset MAC address
- WLAN Handset IP address
- Sequence number
- plus, additional items, based on the message type, as shown in Table 17.

Message example:

```
Jan 1 00:01:26 0090.7a02.2a1b (172.16.0.46) [001a] RStat:
AP 00:40:96:48:1D:0C (-56 dBm), Sent 783523, Recvd
791342, MSnt 245, MRcd 5674, BSnt 43, BRcd 10783, TX
drop 43 (0.0%), TX retry 578 (1.2%), RX retry 1217 (1.6%).
```

Table 17 contains the contents of the syslog messages.

Table 17 Syslog message contents

Syslog message	Contents
Failed Handoff (sent whenever the handset decided to hand off, but failed trying)	Failed AP MAC Failed AP signal strength Current AP MAC Current AP signal strength Failure reason
Successful Handoff	New AP MAC New AP signal strength Old AP MAC Old AP signal strength Reason for handoff Other candidate APS: MAC Signal strength Reason not used
Security Error	AP MAC AP signal strength Security mode Error details (mode dependent)
Call Start	Call type (telephony, OAI, PTT) AP MAC AP signal strength
Call End	AP MAC AP signal strength
Audio stats	AP MAC AP signal strength Payload size (in msec) Payloads sent Payloads received Payloads missed (not received) Payloads missed rate (over last 5 seconds) Payloads late Payloads late rate (over last 5 seconds) Average jitter

Table 17 Syslog message contents

Syslog message	Contents
Audio threshold exceeded (Sent if payloads missed rate or payloads late rate exceeds 2%, or if the average jitter is over 2 msec)	AP MAC AP signal strength Payload size (in msec) Payloads sent Payloads received Payloads missed (not received) Payloads missed rate (over last 5 seconds) Payloads late Payloads late rate (over last 5 seconds) Average jitter
Radio stats	AP MAC AP signal strength Directed packets sent Directed packets received Multicast packets sent Multicast packets received Broadcast packets sent Broadcast packets received TX dropped count TX drop rate (over last 5 seconds) TX retry count TX retry rate (over last 5 seconds) RX retry count RX retry rate (over last 5 seconds)
Radio threshold exceeded (Sent if TX drop rate exceeds 2%, or TX or RX retry rate exceeds 5%)	AP MAC AP signal strength Directed packets sent Directed packets received Multicast packets sent Multicast packets received Broadcast packets sent Broadcast packets received TX dropped count TX drop rate (over last 5 seconds) TX retry count TX retry rate (over last 5 seconds) RX retry count RX retry rate (over last 5 seconds)

Table 17 Syslog message contents

Syslog message	Contents
VPN: Established IKE phase1 SA, renew in xs VPN: Established IKE phase2 SA yy:yy, renew in xs (a phase1 message follows the phase2 message, sent whenever a phase 1 or phase 2 security association completes)	Expiration time and security association identifiers, if applicable. sx is the number of seconds yy:yy stands for the two eight-digit SA numbers for send and receive
VPN: phase2 Unexpected message VPN: phase2 Initiated by VN server VPN: phase2 INFO Delete payload	none

Site certification

Certification must be done to ensure that the wireless handsets are adequately supported by the site.

Conduct a Site Survey of the installation. Note any areas where coverage is conflicting or inadequate. Note any system difficulties and work with the system administrator to determine the cause and possible remedy. See "Conducting an effective site survey" on page 28 for information on conducting a site survey. See "Troubleshooting the handset" on page 121 for clues to possible sources of difficulties.

The testing must be performed in typical operating conditions, especially if heavy loads occur. Generally, organize the test according to area and volume, placing numerous calls to others who can listen while coverage tests are performed. Note any areas with excessive static or clarity problems and report it.

Testing signal strength with the handset

This test can be performed only if the Nortel WLAN IP Telephony system has been installed and configured.

To test signal strength using the wireless handset

1 Test signal strength in the covered area by putting a handset in Site Survey mode, using **Any/ Smry** ESSID.

See "Run Site Survey" on page 95.

Note: The wireless handset remains in Site Survey mode until it is powered off.

2 Walk the entire coverage area while viewing the display, checking for any expected APs or other ESSIDs. See "Detect overlap or conflicts" on page 104 for a discussion on overlaps and conflicts.

3. Change the handset to **MyID/Smry** ESSID mode, and walk the site again, checking that every location has adequate coverage and good channel allocation. See "Detect radio signal coverage" on page 104 for a discussion on coverage.
4. Change the handset to **MyID/Detl** (single AP mode) and walk the site again, checking each AP to ensure that it is configured for the correct data rates, beacon interval, 802.11 options enable, QoS method and security method. See "Confirm supported data rates" on page 104 for a discussion of the configuration.
5. Make any necessary adjustments to the AP locations and configuration, then repeat this procedure, starting at step 1, until the Site Survey shows adequate coverage and the correct configuration at every location.
6. When testing is complete, press **Power Off/End Call** to power off the wireless handset.

Detect radio signal coverage

Use the multiple ESSID mode in the Site Survey function to show the top four APs. Walk the perimeter of the site. The display on the wireless handset shows the top four APs that the wireless handset can contact.

Note any areas that have inadequate dBm readings.

Adequate coverage is when there is one AP with a stronger signal (more than 70 dBm) in all areas.

Good channel allocation is when, at any point, the strongest AP shown is on a different channel than the next best choice.

Detect overlap or conflicts

Use the single ESSID mode in the Site Survey function. Use this information to detect overlaps or conflicts in AP signaling

Make note of any areas that have APs that are in contention for the same channel.

It is preferable that no overlaps exist anywhere in the site. If the Site Survey mode indicates two APs using the same channel, then at least one other AP must be indicated must be indicated at least 10 dBm stronger than the other two APs to prevent channel conflicts.

Confirm supported data rates

Use the Detl soft key to displays details of the specific AP. Use this information to confirm signal strength and supported data rates.

Site Survey notes

Numbers racing across the wireless handset display indicate AP information is being obtained. A Waiting message indicates the system is not configured properly and the wireless handset cannot find any APs.

Walk around the site to determine supported data rates, one AP at a time.

Each data rate (1, 2, 5.5, or 11 Mb/s) supported by the AP is shown. The rates that are in the Basic Rate set (sometimes referred to as "required" rates) are indicated by a 'b' following the rate number. The Supported and Basic data rates should be the same on all APs for the site.

Push-to-talk

The Push-to-talk (PTT) feature allows the WLAN Handset 2211 to operate in a PTT group-broadcast mode like a two-way radio, in addition to the standard telephone operation. The WLAN Handset 2211 supports eight multicast channels with the current channel saved in memory on the wireless handset.

Note: Push-to-talk is not supported on the WLAN Handset 2210 or WLAN Handset 2212.

A PTT call is initiated by pressing the Talk button located on the right side of the WLAN Handset 2211. All WLAN Handset 2211s that are monitoring that channel will hear the transmission.

The two-way radio mode operates on the concept of a PTT session or call period. The PTT call period begins with the first transmission and ends when there has been no two-way radio traffic on the channel for 10 seconds. The PTT mode controls the keypad during a PTT call period. Therefore, it is not possible to use the keypad for any other function such as accessing the on-hook menus or accessing an OAI application. However, it is possible to place a PBX call.

PTT operation

To initiate a PTT call

1. To initiate a PTT call, press and hold the **Talk** button. Wait two seconds to activate the channel before talking.
2. Speak after the “start transmit” sound is heard.

   When the **Talk** button is released, the “end transmit” sound is heard. The WLAN Handset 2211 then enters the waiting state where it monitors the channel for up to 10 seconds.
3. Initiate subsequent transmissions by pressing the Talk button on any WLAN Handset 2211 using the same channel. The “start transmit” sound is played immediately and speech can begin. The display screen shows the current active channel. Since all phones on that channel are already in the receive state, there is no two-second delay.

   If no transmission occurs during the 10-second countdown period, the WLAN Handset 2211 plays the “end call” sound and reverts to the idle state.

Receiving a PTT transmission

Upon receiving a PTT transmission, the WLAN Handset 2211 plays the “receiving alert” sound and enters the “receive” state. In this state, the WLAN Handset 2211 receives all conversations on the selected channel. The WLAN Handset 2211 ignores the Talk key while in the receive state.

The WLAN Handset 2211 screen displays the current active channel, the Caller ID information of the current transmitter, and an indication that the WLAN Handset 2211 is receiving a broadcast transmission. At the end of a transmission, the WLAN Handset 2211 enters the waiting state where it monitors the channel for up to 10 seconds and displays “Waiting” on the screen. If no other transmission occurs within 10 seconds, the WLAN Handset 2211 plays the “end call” sound and reverts to the idle state.

The user can push the Up and Down buttons to raise or lower the volume of the PTT transmission. A separate volume is maintained for PTT calls with the current volume selection retained in memory.

To exit a PTT broadcast, press the Terminate soft key and answer Yes to the confirmation prompt. PTT audio is immediately stopped and the WLAN Handset 2211 exits the PTT session. No other WLAN Handset 2211 is affected. Only the current PTT call is terminated for this WLAN Handset 2211. When another PTT call starts, the WLAN Handset 2211 is again in the receive state. A still-active session can be rejoined by initiating a PTT call.

Disable the PTT feature in the on-hook User Menu to prevent receiving any further PTT calls.

Note: PTT dialog is interrupted when an incoming telephone call is answered. When the telephone call is ended, PTT dialog resumes if an active PTT call is still transmitting.

Interaction with telephone calls

An incoming telephone call can be answered while in a PTT call session. To announce an incoming call, the WLAN Handset 2211 rings with a low-volume ring and displays the system message. To answer the call, press Power On/Start Call. The PTT call session is pre-empted and no PTT audio is heard. After the telephone call is over, press Power Off/End Call as usual to go back on-hook, at which time PTT goes out of the pre-empted mode and becomes active again. If an already active PTT call has not ended, the PTT audio starts playing again.

If the user does not answer the telephone call by pressing Power On/Start Call, the PTT display is shown again after the ring has stopped.

To start a telephone call during a PTT call session, press the Power On/Start Call key. This causes the two-way radio to be pre-empted until the telephone call is ended.

User-defined preferences

The following user-defined preferences can be configured by the wireless handset end-user in the User Option Menu:

- Ring Type
- High Noise Mode
- Current IP Address
- Extension Number Display
- Call Server IP
- Call Server Port
- Terminal Type
- Push To Talk enable/disable

To configure the user-defined options, the wireless handset must be in contact with the system, no error messages displayed, and in Standby mode.

For detailed information on the user-defined preferences in the User Option Menu and how to configure them, refer to the *WLAN Handset 2210/2211/2212 User Guide*.

Configuration cradle worksheet

Complete one copy of this worksheet for each category in the configuration plan before using the Configuration cradle. Label each worksheet with the plan category and filename.

Table 18 Plan Category:_____ Filename: _____

Sys	Grp	Usr	Label	Editable Setting

Chapter 8
Administration and maintenance

Adding a WLAN IP Telephony Manager 2245 to the system

When a WLAN IP Telephony Manager 2245 is added to the system, the change is seamless and does not affect wireless handset calling ability.

A new WLAN IP Telephony Manager 2245 is detected within two seconds of being added to the system (booted/configured/connected). When detected, any wireless handset not on an active call is immediately forced to check out and check in again. Any wireless handset in a call immediately switches to the WLAN IP Telephony Manager 2245 that should provide its “timing” function. This switchover should not be noticeable to the user since it is similar to a normal handoff between APs. When the wireless handset ends the call, it is forced to check out and check in again.

Checking in to the Gateway

When a wireless handset is checking in with the WLAN IP Telephony Manager that is providing the Gateway function (not necessarily the same WLAN IP Telephony Manager 2245 that is providing the timing function), the wireless handset is assigned its Alias IP address. Subsequently when the wireless handset checks in with the LTPS, the wireless handset identifies itself with its new Alias IP address to the Call Server. If the wireless handset is checking in again and again, it may indicate a problem on the network, such as poor AP coverage for a user who is moving about. This information is useful when troubleshooting.

Replacing a WLAN IP Telephony Manager 2245

Failed master WLAN IP Telephony Manager 2245

If the master WLAN IP Telephony Manager 2245 fails, then no telephone calls can be made or received on that subnet. To quickly restore functionality to the wireless telephone network, Nortel recommends changing the configuration of a slave WLAN IP Telephony Manager 2245 to the configuration of the master. Then reset all the other slave WLAN IP Telephony Managers 2245. When they come back up, the slaves recognize the reconfigured slave as the new master.

To replace the failed WLAN IP Telephony Manager 2245 see“To replace a WLAN IP Telephony Manager 2245.

Replacing the failed WLAN IP Telephony Manager 2245

To replace the failed WLAN IP Telephony Manager 2245 see“To replace a WLAN IP Telephony Manager 2245.

To replace a WLAN IP Telephony Manager 2245

1. Disconnect the power cables and LAN cables from the WLAN IP Telephony Manager 2245.
2. Remove the failed device from the wall or rack mount.
3. Mount the replacement device in the same manner as the failed device was mounted.
4. Connect the replacement device to the LAN and power supply.
5. Configure the replacement WLAN IP Telephony Manager 2245.
6. Download the software to the replacement WLAN IP Telephony Manager 2245.
7. Test the replacement device to ensure that it has been installed and configured correctly.

   For detailed information on installing and configuring the WLAN IP Telephony Manager, see "Installing the WLAN IP Telephony Manager 2245" on page 48 and "WLAN IP Telephony Manager 2245 configuration" on page 51.

Removing a WLAN IP Telephony Manager 2245 from the system

When a WLAN IP Telephony Manager 2245 is removed from the system, wireless handsets using the WLAN IP Telephony Manager 2245 are affected. If the removal of the WLAN IP Telephony Manager 2245 is intentional, lock and idle the system before removing a WLAN IP Telephony Manager 2245.

When a WLAN IP Telephony Manager 2245 is removed from the system, the removal is detected within two seconds. Wireless handsets not in calls are immediately forced to check out and check in again.

Wireless handset scenarios

For wireless handsets on active calls, two possible scenarios can occur.:

- If the removed WLAN IP Telephony Manager 2245 was providing the "gateway" function for the wireless handset, then the call is lost and the wireless handset is forced to check in again.
- If the removed WLAN IP Telephony Manager 2245 was providing the "timing" function for the call, the call switches to the WLAN IP Telephony Manager 2245 that should now provide the "timing" function.

Note: During the two seconds while the loss of the WLAN IP Telephony Manager 2245 is being detected, the audio for the call is lost.

Changing the master WLAN IP Telephony Manager 2245

If the master WLAN IP Telephony Manager 2245 loses communication with the network, the wireless telephone system fails. All WLAN IP Telephony Managers 2245 lock. All calls are lost and no calls can be placed.

Therefore, if the master WLAN IP Telephony Manager 2245 must be replaced, ensure the system can be shut down with minimal call interruption. Reset all WLAN IP Telephony Managers 2245 after the master has been replaced. If the IP address of the master WLAN IP Telephony Manager 2245 is changed, the new IP address must be re-configured in all WLAN IP Telephony Managers 2245 using that master.

Viewing software version

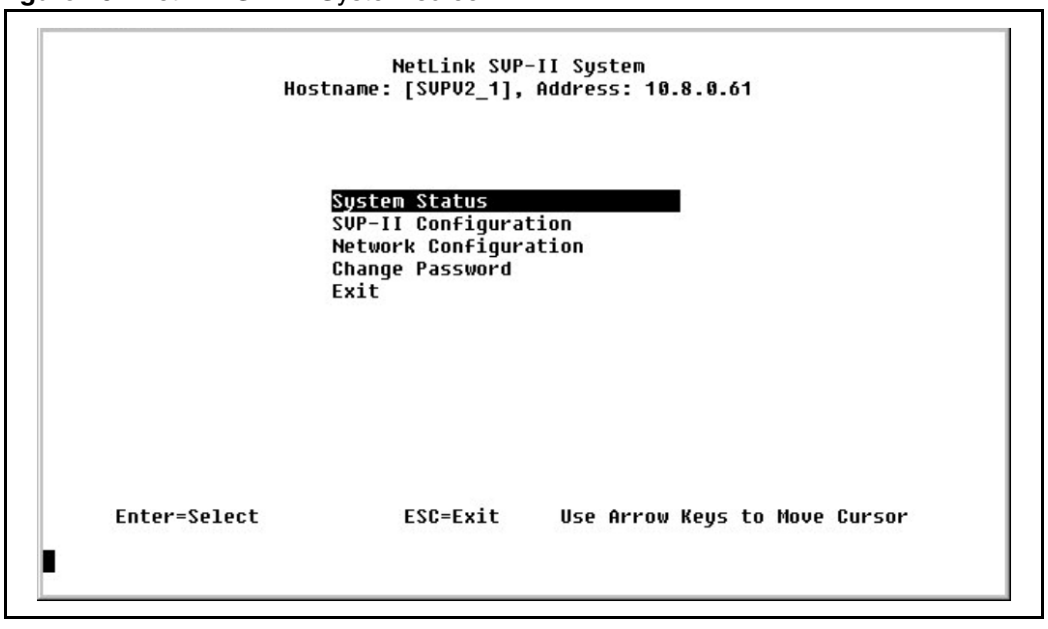
For the WLAN IP Telephony Manager 2245

To view the software versions for the WLAN IP Telephony Manager 2245, follow the steps in "To view the software version" on page 111.

To view the software version

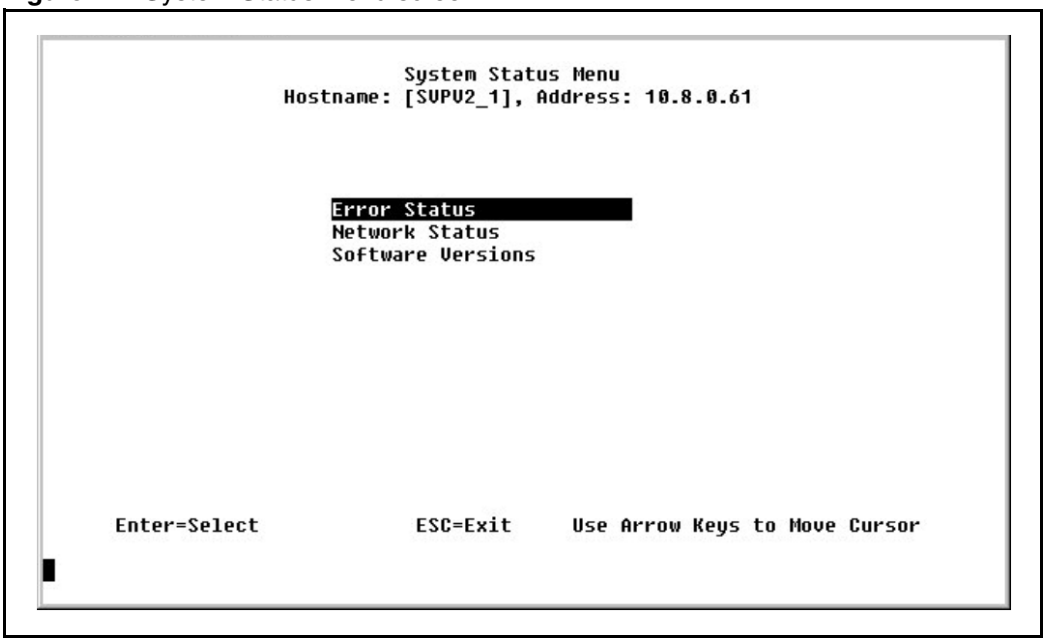
1 From the WLAN IP Telephony Manager 2245's **NetLink SVP-II System** screen, select **System Status** and press **Enter**. See Figure 16.

Figure 16 NetLink SVP-II System screen



The System Status Menu screen appears. See Figure 17 on page 112.

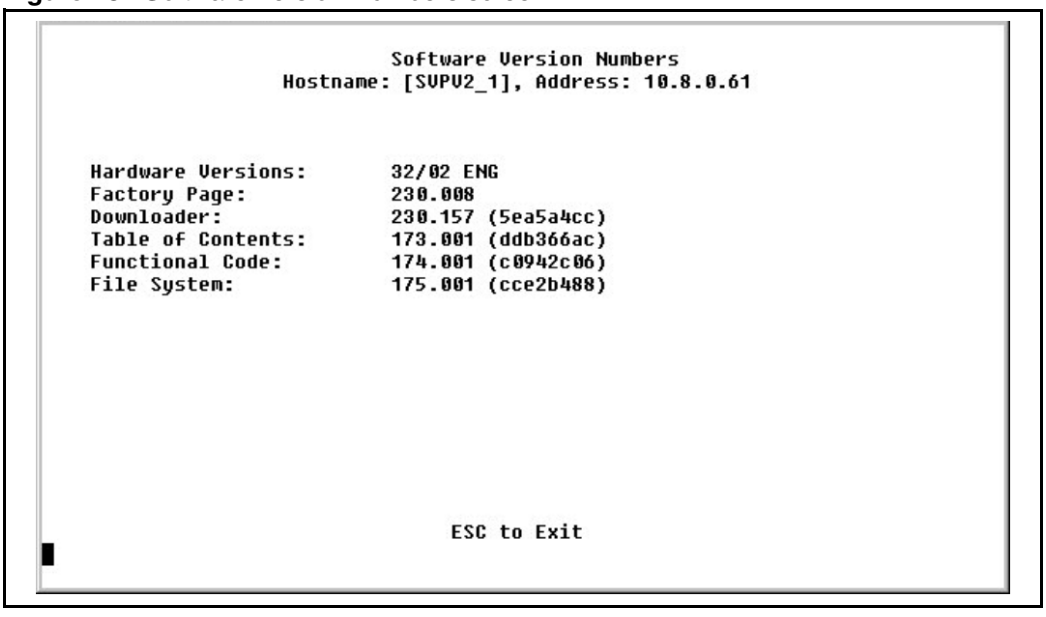
Figure 17 System Status Menu screen



2 Scroll down to **Software Versions** and press **Enter**.

Result: The Software Version Numbers screen appears. See Figure 18. The software version for each WLAN system component is displayed. The current software version numbers may vary from the example shown.

Figure 18 Software Version Numbers screen



For the WLAN Application Gateway 2246

For information on viewing the software versions for the optional WLAN Application Gateway 2246, see Appendix A, "WLAN Application Gateway 2246.

For a wireless handset

The software versions running on the wireless handsets can be displayed by powering on the wireless handset and holding down the Power On/Start Call key

Updating software

Nortel provides information about software updates. Download the software updates from www.nortel.com.

After obtaining the software updates from Nortel, transfer them to the TFTP Server accessed by the WLAN IP Telephony Manager 2245.

Updating software on the WLAN IP Telephony Manager 2245

To update the software on the WLAN IP Telephony Manager 2245, reset it. When the WLAN IP Telephony Manager 2245 starts up, it compares its software version to the software version on the TFTP Server. The WLAN IP Telephony Manager 2245 downloads the software from the TFTP Server if the versions are different.

CAUTION

Always ensure that only the latest version of software is on the TFTP Server and that earlier software versions are deleted, moved, or renamed.

At startup, the WLAN IP Telephony Manager 2245 always uses TFTP to compare its software version with the version on the TFTP Server. If the versions are different, the WLAN IP Telephony Manager 2245 downloads the software version from the TFTP Server, even if it is an older version.

Locking the system

Always lock the WLAN IP Telephony Manager 2245 in the SVP-II Configuration screen before updating the software. Locking the WLAN IP Telephony Manager 2245 prevents new calls from starting.

Reset the WLAN IP Telephony Manager 2245 after the update is complete.

Note: All calls in progress are terminated when the WLAN IP Telephony Manager 2245 is reset.

Updating software on the WLAN Application Gateway 2246

For information on updating the software on the optional WLAN Application Gateway 2246, see Appendix A, “WLAN Application Gateway 2246.

Updating software on a wireless handset

The WLAN system allows over-the-air transfer of software updates from the designated TFTP Server to the wireless handsets.

The downloader function in the wireless handset checks its software version every time the wireless handset is turned on. If there is any difference in the software version, the wireless handset immediately begins to download the update.

On a clear 802.11a/b/g channel, the download process takes one minute or less to complete.

If the TFTP Server cannot be reached at the time the wireless handset is powered on, resets, or comes back into a WLAN service area, the wireless handset tries a few times to contact the TFTP Server, then gives up and uses the existing software.

If more wireless handsets are requesting TFTP service than the TFTP Server has ports available, or if the TFTP Server is unreachable or unavailable, the wireless handsets try a few times to reach the TFTP Server, then continue to use the existing software. In other words, it is not possible to guarantee that a wireless handset is using the latest software. For example, it is not possible to guarantee that all wireless handsets are upgraded as a result of an isetResetAll command. To verify that a wireless handset is running the intended version of software, use the isetShow command to determine the software version.

From the Signaling Server or Voice Gateway Media Card, use the oam> or IPL> isetGet command to display a list of all currently registered wireless handsets that are running the old firmware version. Use this command on all LTPS Signaling Servers or Voice Gateway Media Cards that have IP Phones and wireless handsets currently registered:

oam> isetGet fwvsn==<old 2210/2211/2212 firmware version>

Displays

When the wireless handset is powered on, it displays a series of messages indicating that it is searching for new software, checking the versions, and downloading the software. During the download, a progress bar on the wireless handset display screen displays the progress of the download.

IMPORTANT!

While the wireless handset is updating the software, the NO SVC message displays, and the wireless handset should not be powered off. For approximately 10 seconds, the wireless handset cannot be powered off. A warning message is displayed during that time. If the warning message is not displayed, the wireless handset can be powered off without damage.

When the update is complete, the wireless handset displays the extension number, and is ready for use.

Wireless handset download messages

Normal download messages

When the wireless handset is powered on, it displays a series of messages indicating that it is searching for new software, checking the software versions, and downloading. The normal message progression is listed in Table 19.

Table 19 Normal download messages

Message	Description
Checking Code	Wireless handset is contacting the TFTP Server to determine if the server has a newer version of software that should be downloaded.
Erasing Memory	Wireless handset has determined that a download should occur and is erasing the current software from memory. This message also displays a progress bar. When the progress bar fills the display line, the erase operation is complete.
Updating Code	Wireless handset is downloading new software into memory. This message also displays a progress bar. When the progress bar fills the display line, the update operation is complete on that file.

When the update is complete, the wireless handset displays the extension number, and is ready for use.

Download failure or recovery messages

Table 20 lists the display messages for the wireless handset that indicate a failure or recovery situation during the software download process.

Table 20 Failure and recovery messages

Message	Description
Server Busy	Wireless handset is attempting to download from a TFTP Server that is busy downloading other handsets and refusing additional downloads. The wireless handset automatically retries the download every few seconds.
TFTP Error (x):yy	A failure occurred during the TFTP download of one of the files. **(x)** = the file number that was being downloaded. **yy** = an error code describing the particular failure. Possible error codes are: 01 = TFTP Server did not find the requested file. 02 = Access violation (reported from TFTP Server). 07 = TFTP Server reported “No such user” error. Check the TFTP Server configuration. 81 = File put into memory did not CRC. The wireless handset attempts to download the file again. FF = Timeout error. TFTP Server did not respond within a specified period of time.
Erase Failed	Download process failed to erase the memory in the wireless handset. This operation retries.
Waiting	Wireless handset has attempted an operation several times and failed, and is now waiting for a period of time before attempting that operation again.
Internal Error OE	OE = Error while writing the Flash (return wireless handset to Nortel).

Chapter 9
Troubleshooting

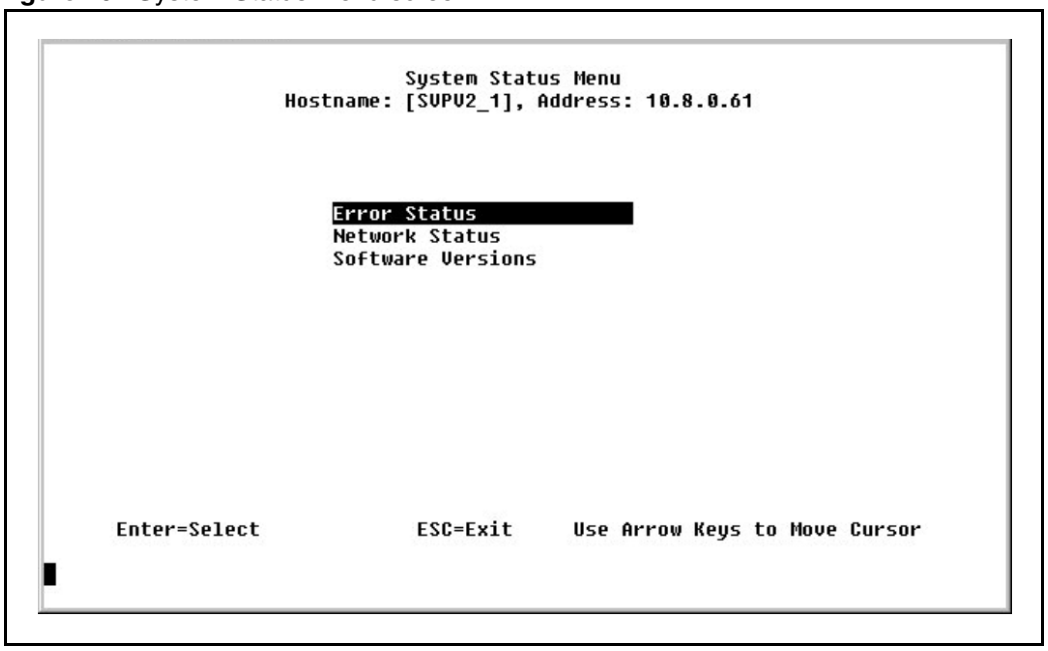
Troubleshooting the WLAN IP Telephony Manager 2245

Information about system alarms and network status is obtained through the System Status Menu screen. For information on how to connect to the WLAN IP Telephony Manager 2245 and access the System Status Menu screen from the NetLink SVP-II System screen, see "WLAN IP Telephony Manager 2245 configuration" on page 51.

Options on the System Status Menu screen provide a window into the real-time operation of the system's components. Use this data to evaluate system function and to troubleshoot areas that may be experiencing problems.

The System Status Menu screen is shown in Figure 19.

Figure 19 System Status Menu screen



The following options can be selected:

- **Error Status** – displays alarm and error message information.
- **Network Status** – displays information about the Ethernet network to which the WLAN IP Telephony Manager 2245 is connected.
- **Software Versions** – lists the software versions for the WLAN IP Telephony Manager 2245.

Error Status screen

The Error Status screen displays any alarms that indicate some system malfunction. Some of these alarms are easily remedied. Others require a call to Nortel Technical Support.

From the System Status Menu screen, select Error Status. The Error Status screen displays active alarms on the WLAN IP Telephony Manager 2245. Table 21 lists the alarms and the actions required to eliminate the alarm.

Table 21 WLAN IP Telephony Manager 2245 active alarms and actions

Alarm text	Action
Maximum payload usage reached	Reduce usage, clear alarm
Maximum telephone usage reached	Reduce usage, clear alarm
Maximum Access Point usage reached	Reduce usage, clear alarm
Maximum call usage reached	Reduce usage, clear alarm
SRP audio delayed	Reduce usage, clear alarm
SRP audio lost	Reduce usage, clear alarm
No IP address	Configure an IP address

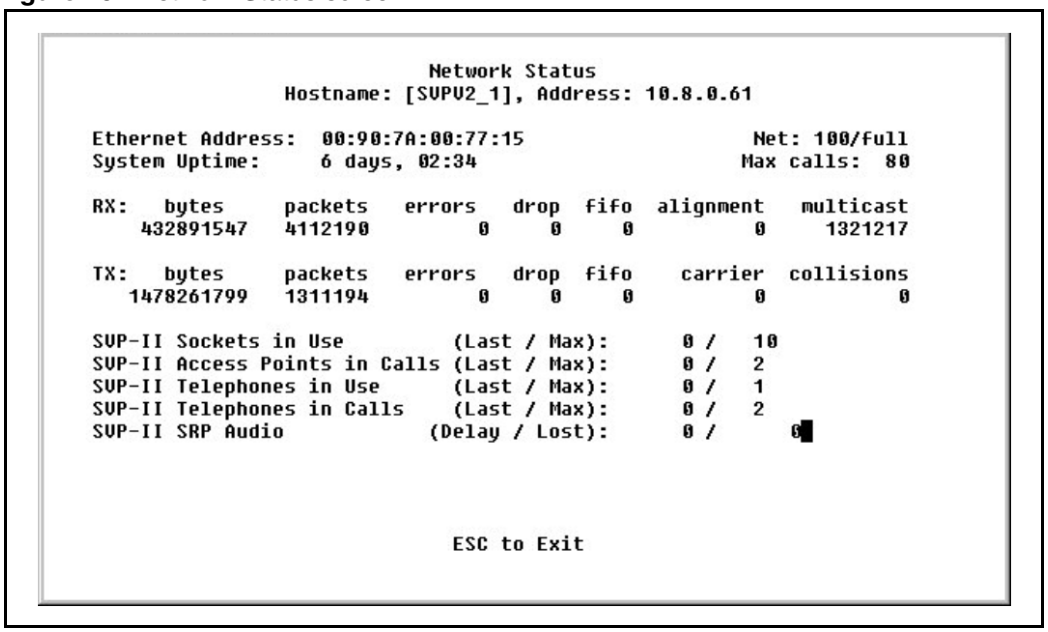
Press **C** to clear all clearable alarms.

Network Status screen

The WLAN IP Telephony Manager 2245 is connected to the Ethernet network (LAN). The information about that connection is provided on the Network Status screen. The screen displays information about the Ethernet network. This information can help troubleshoot network problems.

To access the Network Status screen, select Network Status from the System Status Menu screen. The Network Status screen is shown in Figure 20 on page 119.

Figure 20 Network Status screen


Network Status
Hostname: [SVPV2_1], Address: 10.8.0.61
Ethernet Address: 00:90:7A:00:77:15
Net: 100/full
System Uptime: 6 days, 02:34
Max calls: 80
RX: bytes packets errors drop fifo alignment multicast
432891547 4112190 0 0 0 0 1321217
TX: bytes packets errors drop fifo carrier collisions
1478261799 1311194 0 0 0 0 0
SVP-II Sockets in Use (Last / Max): 0 / 10
SVP-II Access Points in Calls (Last / Max): 0 / 2
SVP-II Telephones in Use (Last / Max): 0 / 1
SVP-II Telephones in Calls (Last / Max): 0 / 2
SVP-II SRP Audio (Delay / Lost): 0 / 0
ESC to Exit

The following information can be viewed:

- **Ethernet Address** – MAC address of the WLAN IP Telephony Manager 2245 (hexadecimal).
- **System Uptime** – the number of days, hours, and minutes since the WLAN IP Telephony Manager 2245 was last reset.
- **Net** – the type of connection to the Ethernet switch currently utilized. Displayed as 10 (10BaseT) or 100 (100BaseT)/half-duplex, full-duplex, or auto-negotiate.
- **Max (maximum) calls** – number of calls that can be supported by the WLAN IP Telephony Manager 2245 (depends on network speed).
- **RX** – Ethernet statistics about the received signal during System Uptime.
  - bytes – number of bytes received
  - packets – number of packets received
  - errors – sum of all receive errors (long packet, short packet, CRC, overrun, alignment)
  - drop – packets dropped due to insufficient memory
  - fifo – overrun occurred during reception
  - alignment – non-octet-aligned packets (number of bits not divisible by 8)
  - multicast – packets received with a broadcast or multicast destination address
- **TX** – Ethernet statistics about the transmitted signal during System Uptime.
  - bytes – number of bytes transmitted
  - packets – number of packets transmitted
  - errors – sum of all transmit errors (heartbeat, late collision, repeated collision, underrun, carrier)
  - drop – packets dropped due to insufficient memory

- fifo – underrun occurred during transmission
- carrier – count of carrier losses during transmission
- collisions – packets deferred (delayed) due to collision

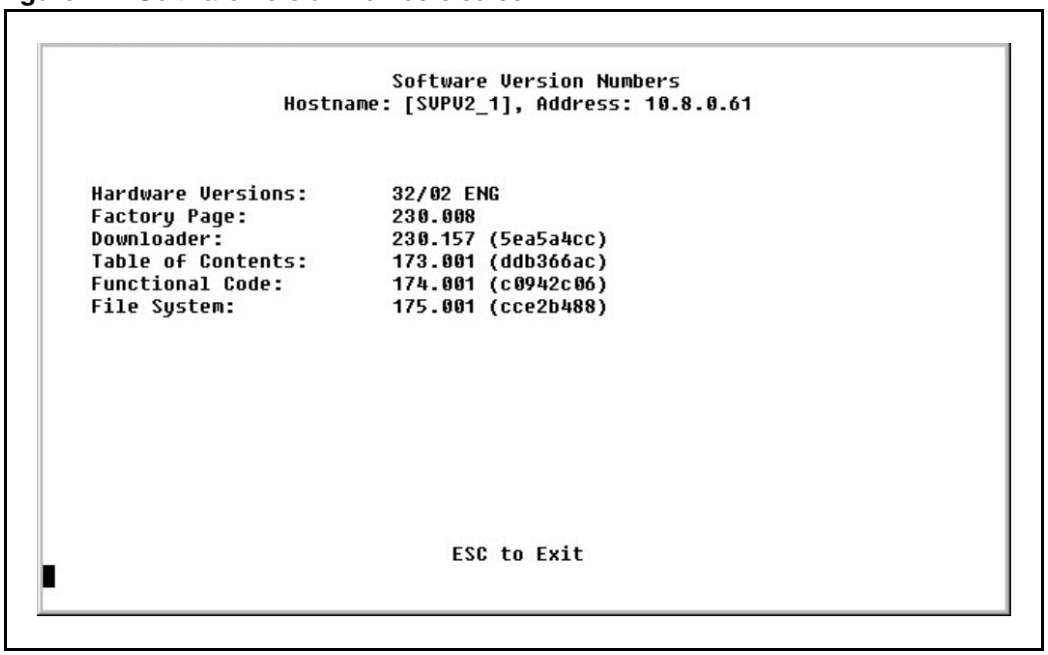
- **SVP-II Access Points in Use** – number of APs in use by wireless handsets, either in standby or in a call. **Last** is current use, **Max** is the maximum number in use at one time.
- **SVP-II Access Points in Calls** – number of APs with wireless handsets in a call.
- **SVP-II Telephones in Use** – number of wireless handsets in standby or in a call.
- **SVP-II Telephones in Calls** – number of wireless handsets in a call.
- **SVP-II SRP Audio**
  - Delay – SRP audio packets whose transmission was momentarily delayed
  - Lost – SRP audio packets dropped due to insufficient memory resources

Software Version Numbers screen

The Software Version Numbers screen provides information about the software version currently running on the WLAN IP Telephony Manager 2245.

This information helps to determine if the most recent software version is running. This information assists Nortel Technical Support in troubleshooting software problems.

Figure 21 Software Version Numbers screen



Speed or duplex mismatch

A duplex mismatch on the WLAN can cause the WLAN IP Telephony Manager 2245 to not operate properly. Double-check WLAN connections and interfaces to ensure that they are all configured as full-duplex.

In rare instances, the message “Speed or Duplex mismatch error” can occur during the boot-up sequence of the IP Telephony Manager 2245.

If this situation occurs, verify all devices connected to the WLAN IP Telephony Manager 2245 are configured correctly and no duplex mismatch is found. If all configurations are correct, reboot the IP Telephony Manager 2245. The error message should be cleared.

Troubleshooting the WLAN Application Gateway 2246

For information on troubleshooting the optional WLAN Application Gateway 2246, see Appendix A, “WLAN Application Gateway 2246.

Troubleshooting the handset

Wireless handsets can exhibit transmission problems in several ways. They can cease functioning properly, display error messages, or display incorrect data. When using and troubleshooting wireless handsets, consider the following problem sources to determine the best method of approaching a specific situation.

Context

When troubleshooting a problem with a wireless handset, it is important to determine the context of when and where the problem occurred. Context includes the following:

- Was the wireless handset on an active call?
- Was the wireless handset moving or stationary?
- Was the wireless handset powering on or powering off?
- Was PTT being used?
- At what location did the problem occur?

Record this information and provide it to the system administrator or Nortel Technical Support.

Access Point problems

Most, but not all, wireless handset audio problems are related to AP range, positioning, and capacity. Performing a Site Survey as described in “Site survey” on page 25 can isolate the AP causing these types of problems. If the wireless handset itself is suspected, conduct a parallel site survey with a wireless handset that is known to be functioning properly.

The following are some situations that can cause wireless handset difficulties to occur:

- **In range/Out of range** – service is disrupted if a user moves outside the area covered by the WLAN APs. Service is restored if the user moves back within range. If a call drops because a user moves out of range, the wireless handset recovers the call if the user moves back into range within a few seconds.
- **Capacity** – in areas of heavy use, the call capacity of a particular AP may be filled. If this happens, the user hears three chirps from the wireless handset. The user can wait until another user terminates a call, or move within range of another AP and try the call again. If a user is on a call and moves into an area where capacity is full, the system attempts to find another AP. Due to range limitations, this may be the same as moving out of range.
- **Transmission Obstructions –** before system and AP installation, the best location for APs for optimum transmission coverage was determined when a site survey was performed. However, small pockets of obstruction may still be present, or obstructions may be introduced into the facility after AP installation. This loss of service can be restored by moving out of the obstructed area, or by adding more APs.

Configuration problems

Certain problems are associated with improper configuration of either the WLAN IP Telephony 2245, the optional WLAN Application Gateway 2246, or the wireless handset.

Configuration problems are generally corrected by changing the configuration on the WLAN IP Telephony 2245, the WLAN Application Gateway 2246, or the wireless handset.

There may also be incorrect programming of the APs. See Appendix B, “Compatible Access Points for compatibility and configuration information about the APs in use at the site.

Duplex mismatch

A duplex mismatch on the WLAN can cause the wireless handsets to not operate properly. Double-check WLAN connections and interfaces to ensure that they are all configured as full-duplex.

No ring

It is possible in certain situations for a voice mail message to be left on a wireless handset without the wireless handset ever ringing. This situation could occur when a wireless handset is out of range of an AP for even a few seconds. If during the time the wireless handset were out of AP range and an incoming call was received, the incoming call receives the CFNA treatment configured for that wireless handset, such as forwarding the incoming call to voice mail.

To prevent this situation from occurring, ensure adequate AP coverage in all areas where a wireless handset might be used.

Far-end echo

Sometimes, when using the G.711 codec, echo might be perceptible at the far end, and be more severe when the wireless handset is in an environment with extreme background noise and the wireless handset volume is set to maximum volume.

To correct this problem, reduce the volume setting on the wireless handset. Alternatively, if experiencing this problem, consider using the G.729 codec.

Dropped calls

If calls are dropping, use the Site Survey mode of the wireless handset in the area where the problem occurred to determine if there is inadequate AP coverage in that area.

Wireless handset status messages

Wireless handset status messages provide information about the handset communication with the AP and Call Server. Table 22 summarizes the status messages, in alphabetical order.

Table 22 Wireless handset status messages

Message	Description	Action
3 chirps	Wireless handset is not able to communicate with the best AP, probably because that AP has no bandwidth available.	None. This is only a warning. The call will handoff to the best AP once it becomes available.
Address Mismatch	Wireless handset software download files are incorrect or corrupted.	Download new software from the Nortel site (see "Updating software" on page 113).
ASSERT xxx.c Line yyy	The handset has detected a fault from which it cannot recover.	Record the error information so that it can be reported. Turn the handset off, then on again. If error persists, try registering a different handset to this telephone port. If error still persists, contact Nortel Technical Support and report the error.
Assoc Failed xxxxxxxxxxxx	x…x = AP MAC address Handset association was refused by the AP; displays the MAC of the failing AP.	Check the handset and AP security settings. Ensure that the AP is configured per Configuration Note. Try another AP.
Assoc Timeout xxxxxxxxxxxx	x…x = AP MAC address Handset did not receive an association response from the AP; displays the MAC of the failing AP.	Check the handset and AP security settings. Ensure that the AP is configured per Configuration Note. Try another AP.

Table 22 Wireless handset status messages

Message	Description	Action
Auth Failed xxxxxxxxxxxx	x…x = AP MAC address Handset authentication was refused by the AP; displays the MAC of the failing AP.	Check the handset and AP security settings. Ensure that the AP is configured per Configuration Note. Try another AP.
Auth Timeout xxxxxxxxxxxx	x…x = AP MAC address Handset did not receive an authentication response from the AP; displays the MAC of the failing AP.	Check the handset and AP security settings. Ensure that the AP is configured per Configuration Note. Try another AP.
Bad Code Type xx Expected Code Type yy	xx, yy = software license types Handset software does not match the current handset license selection.	Download new software from the Nortel site (see “Updating software” on page 113).
Bad Config	Some needed configuration parameter has not been set.	Check all required wireless handset configuration parameters for valid settings.
Bad ESSID	The wireless handset is configured for “static ESSID” (as opposed to “Learn once” or “Learn always”) and no ESSID has been entered.	Enter an ESSID in the configuration settings or change to one of the “Learn” modes.
Bad Local ID	The value of the Phase 1 Local ID type entered in the handset through the menus or the configuration cradle is improperly configured.	Enter a valid ID value.
Bad Local ID Type	The Phase 1 Local ID type entered in the handset through the menus or the configuration cradle is missing or invalid.	Enter a valid ID type. KEY ID is the only valid choice.
Bad Network IP	The value of the Remote Network IP address entered in the handset through the menus or the configuration cradle is missing or invalid.	Enter a valid remote network IP address.
Bad Network Mask	The value of the Remote Network network mask entered in the handset through the menus or the configuration cradle is missing or invalid.	Enter a valid network mask.
Bad Payload Type	The VPN server is not accepting some of the parameters passed to it by the handset. One common instance would be it two handsets try to use the Client IP.	If the VPN Client IP is statically configured, ensure that the address assigned to the handset is unique. If using IKE Mode Config, ensure that the address entered in the VPN Server configuration for the handset or user is unique.

Table 22 Wireless handset status messages

Message	Description	Action
Bad Phintl File	The handset software download files are incorrect or corrupted.	Download new software from the Nortel site (see "Updating software" on page 113).
Bad Program File	The handset software download files are incorrect or corrupted.	Download new software from the Nortel site (see "Updating software" on page 113).
Bad Preshared Key	The value of the pre-shared key entered in the handset through the menus or configuration cradle is improperly configured.	Enter a valid pre-shared key value. For a Contivity VPN server, this would be the password.
Bad Tunneled IP	The value of the VPN Client IP address entered in the handset through the menus or the configuration cradle is configured for static IP and is missing.	Enter a valid client IP address.
Bad VPN Server IP	The VPN Server IP address entered in the handset through the menus or the configuration cradle is invalid.	Enter the IP address of the VPN server.
(battery icon), Low Battery message, and beep Battery Low	Low battery	**In call**: the battery icon displays and a soft beep is heard when the user is on the wireless handset and the battery charge is low. User has 15–30 minutes of battery life left. The **Battery Low** message indicates that the battery pack can be changed while the call is still in progress. Do not press **Power Off/End Call**. Place the call on Hold or Park, quickly remove the discharged battery and replace with a charged battery, power on the handset and press **Power On/Start Call** to resume the call in progress. **Not in call**: The battery icon displays whenever the battery charge is low. The message **Low Battery** and a beep indicate a critically low battery charge when user is not on the wireless handset. The wireless handset will not work until the battery pack is charged.
Battery Failure	The battery pack is not functioning.	Replace the battery pack with a new or confirmed battery pack. Only the approved battery pack will work.

Table 22 Wireless handset status messages

Message	Description	Action
Battery Failed	Battery pack is damaged or incompatible with the handset.	Replace the battery pack with a new or confirmed battery pack. Only the approved battery pack will work.
Can't renew DHCP yyy.yyy.yyy.yyy	y…y = DHCP server IP address DHCP server is not responding to the initial renewal attempt.	Configuration problem. Check the IP address configuration in the DHCP server.
Charging …	The wireless handset is charging in the Desktop Charger.	No action needed.
Charge Complete	The wireless handset is now fully charged.	No action needed.
Checking Code	Wireless handset is contacting the TFTP Server to determine if it has a newer version of software that should be downloaded.	None. This message should only last for approximately one second. If message remains displayed, power off and contact Nortel Technical Support.
Checking DHCP IP	The wireless handset is retrieving DHCP information from the DHCP server.	None. This is for information only.
CRC Code Error	The software that has been TFTP downloaded has a bad Cyclical Redundancy Code (CRC) check.	Try the download again. It is possible the software was corrupted during download. If the error repeats, check that the download image on the TFTP Server is not corrupted.
Code Mismatch!	The software loaded into the wireless handset is incorrect for this model of telephone.	Verify that the License Management value is correct. Replace the software image on the TFTP server with software that is correct for the handset model.
DCA Timeout	The handset has detected a fault from which it cannot recover, possibly due to a failure to acquire any network.	Turn the handset off, then on again. If the error persists, contact Nortel Technical Support and report the error.

Table 22 Wireless handset status messages

Message	Description	Action
DHCP Error (1-5)	DHCP Error 1	The wireless handset cannot locate a DHCP server. It will try every 4 seconds until a server is located.
	DHCP Error 2	The wireless handset has not received a response from the DHCP server to a request for an IP address. It will retry until a DHCP server is found.
	DHCP Error 3	The server refuses to lease the wireless handset an IP address. It will keep trying.
	DHCP Error 4	The DHCP server offered the wireless handset a lease that is too short. The minimum lease time is 10 minutes. One hour is the minimum recommended lease time. The wireless handset will stop trying. Reconfigure the DHCP server and power-cycle the wireless handset.
	DHCP Error 5	Failure during WEP Key rotation process (proprietary failure).
DHCP Lease Exp yyy.yyy.yyy.yyy	y…y = DHCP Server IP address DHCP is not responding to renewal attempts. At least one renewal succeeded.	The wireless handset failed to renew its DHCP lease, either because the DHCP server is not running, or because the configuration has been changed by the administrator. The wireless handset will attempt to negotiate a new lease or display one of the DHCP errors (1-5).
DHCP NACK error yyy.yyy.yyy.yyy	y…y = DHCP Server IP address DHCP server explicitly refused renewal.	The DHCP lease currently in use by the wireless handset is no longer valid, which forces the wireless handset to restart. This problem should resolve itself on the restart. If it does not, the problem is in the DHCP server.
DL Not On Sector	The handset software download files are incorrect or corrupted.	Download new software from the Nortel site (see "Updating software" on page 113).
DO NOT POWER OFF	The wireless handset is in a critical section of the software update.	None. Do not remove the battery or attempt to power off the phone while this message is displayed. Doing so may require the wireless handset to be returned to Nortel to be recovered.

Table 22 Wireless handset status messages

Message	Description	Action
Duplicate IP	The wireless handset has detected another device with its same IP address.	If using DHCP, check that the DHCP server is properly configured to avoid duplicate addresses. If using Static IP, check that the wireless handset was assigned a unique address.
Erase Failed	Download process failed to erase the memory in the wireless handset.	Operation will retry but may eventually report the error “int. error: 0F”. Power cycle the wireless handset.
Erasing memory	The wireless handset has determined that a download should occur and is erasing the current software from memory.	None. When the progress bar fills the display line, the erase operation is complete. Note: Do not turn the handset off during this operation.
Files Too Big	The handset software download files are incorrect or corrupted.	Download new software from the Nortel site (see “Updating software” on page 113).
Flash Config Error	Handset internal configuration is corrupt.	Perform the “Restore Defaults” operation from the administrator menu and reprogram, or reprogram using the configuration cradle.
Initializing …	The wireless handset is performing a power-on initialization.	None. This is informational only.
Internal Err. # #	The wireless handset has detected a fault from which it cannot recover. OE=Error while writing the Flash (return handset to factory) OF = No functional code (contact Nortel Technical Support)	Record the error code so it can be reported. Turn the wireless handset off, then on again. If error persists, try registering a different wireless handset to this telephone port. If error still persists, contact Nortel Technical Support and report the error.
Invalid ID Info	The VPN server did not recognize this user.	Make sure that the local ID (KEY ID) entered in the handset matches the key Id in the VPN server. For a Contivity VPN server, the local ID must match the username.

Table 22 Wireless handset status messages

Message	Description	Action
Multiple SVP Svr yyy.yyy.yyy.yyy	y…y = WLAN IP Telephony Manager 2245 IP address Handset received responses from multiple WLAN IP Telephony Managers 2245; displays the IP address of one responding WLAN IP Telephony Manager 2245.	Happens if the handset has been reconfigured to use a different WLAN IP Telephony Manager 2245 and then powered-down before the previous server has had time to determine that the handset is no longer connected to it. The problem should correct itself in about 30 seconds.
Must upgrade SW!	Handset software is incompatible with the hardware.	Download new software from the Nortel site (see "Updating software" on page 113).
Net Busy xxxxxxxxxxxx	x…x = AP MAC address Handset cannot obtain sufficient bandwidth to support a call; displays the MAC of the failing AP.	Try call again later.
No DHCP Server	Handset is unable to contact the DHCP server.	Check that DHCP is operational and connected to the WLAN or use Static IP configuration in the handset.
No ESSID	Attempted to run the site survey application without an ESSID set.	Let the handset come completely up. Statically configure an ESSID in the Admin menu.
No Func Code	Handset software download files are incorrect or corrupt.	Reconfigured the handset to gain access to the WLAN and download new code.
No Host IP (Addr)	The wireless handset is configured for "static IP" (as opposed to "use DHCP") and no valid host IP address (the wireless handset IP address) has been entered.	Enter a valid IP address in the configuration settings or change to "use DHCP."
No IP Address	Invalid IP address.	Check the IP address of the wireless handset and reconfigure if required.
No Net Access	Cannot authenticate/associate with AP.	Verify the AP configuration. Verify that all the WEP settings in the handset match those in the APs.

Table 22 Wireless handset status messages

Message	Description	Action
No Net Found	This indicates any of the following:	
	No radio link	Verify that the AP is turned on.
	No ESSID — Autolearn not supported (or) incorrect ESSID	Verify the ESSID of the wireless LAN and enter or Autolearn it again, if required.
	AP does not support appropriate data ranges	Check the AP configuration against the AP Configuration Note.
	Out of Range	Try getting closer to an AP. Check to see if other handsets are working within the same range of an AP. If so, check the ESSID of the handset.
	incorrect WEP settings	Verify that all the WEP settings in the handset match those in the APs.
	Incorrect Security settings	Verify that all the Security setting in the AP.
No Net Found xxxxxxxxxxxx yy	x…x = AP MAC address yy = AP signal strength Handset cannot find a suitable AP; displays the MAC address and signal strength of the “best” non-suitable AP found.	Check the AP and handset network settings, such as ESSID, Security, Reg. domain and Tx power. Ensure that the APs are configured per Configuration Note. Try Site Survey mode to determine a more specific cause.
No PBX Response	The wireless handset tried to send a message to the Call Server and failed to get a response.	Verify the Call Server is operational and connected to the network.
No Proposal	The handset and the VPN server could not agree on a set of configuration parameters.	Check that the Diffie-Hellman group, phase 1and phase 2 hashes, and the encryption algorithms configured on the handset are acceptable to the VPN server.
No Reg Domain	Regulatory Domain not set	Configure the Regulatory Domain of the handset.
No SVP IP	The wireless handset is configured for “static IP” (as opposed to “use DHCP”) and no valid WLAN IP Telephony Manager 2245 address has been entered.	Enter a valid WLAN IP Telephony Manager 2245 IP address in the wireless handset’s configuration setting or change to “use DHCP.”

Table 22 Wireless handset status messages

Message	Description	Action
No SVP Response yyy.yyy.yyy.yyy	y…y = SVP Server IP address The handset has lost contact with the WLAN IP Telephony Manager 2245.	This may be caused by bad radio reception or a problem with the WLAN IP Telephony Manager 2245. The handset keeps trying to fix the problem for 20 seconds, and the message may clear by itself. If it does not, the handset restarts. Report this problem to the system administrator if it keeps happening.
No SVP Server	Wireless handset can't locate WLAN IP Telephony Manager 2245.	IP address configuration of WLAN IP Telephony Manager 2245 is wrong or missing.
	WLAN IP Telephony Manager 2245 is not working.	Check error status screen on WLAN IP Telephony Manager 2245.
	No LAN connection at the WLAN IP Telephony Manager 2245.	Verify WLAN IP Telephony Manager 2245 connection to LAN.
No SVPServer No DNS Entry	The handset was unable to perform DNS lookup for the WLAN IP Telephony Manager 2245; server had no entry for SVP Server.	The network administrator must verify that a proper IP address has been entered for the SVP Server DHCP option.
No SVPServer No DNS IP	The handset was unable to perform a DNS lookup for the WLAN IP Telephony Manager 2245; no IP address for DNS server.	The network administrator must verify proper DHCP server operation.
No SW Found	A required software component has not been properly identified.	Check that the handset license type has a corresponding entry in the slink_cfg.cfg file. Check that the pd11ccc.bin and pi110003.bin entries exist under this type in the slnk_cfg.cfg.
No UNIStim DHCP	The handset was unable to use DHCP to obtain the server information it needs to start up.	Verify the DHCP server configuration information. Verify network connectivity between the handset and the DHCP server.
No VPN Server	The handset could not find the VPN server.	Check that the value of the VPN Server IP address configured through the administration menu or the configuration cradle match the address of the VPN server.

Table 22 Wireless handset status messages

Message	Description	Action
Not Installed!	A required software component is missing.	Check that all required software files are on the TFTP Server, if over-the-air downloading is being used. If the error repeats, contact Nortel Technical Support.
Payload Malfmd	The handset could not understand an encrypted message from the VPN Server (or vice-versa). This is likely to be a mismatch in the security parameters such as preshared key, Diffie-Hellman group, hash and encryption algorithms.	Check the Diffie-Hellman group, the phase 1 and phase 2 hashes, and encryption configuration.
Press End Call	The call has ended.	Press the Power Off/End Call key to return to standby mode.
Restart Command	The wireless handset received a restart command from the Call Server.	None. The wireless handset will automatically restart in a few seconds.
RTP Open Failed	The handset was unable to open the requested RTP or RTCP socket.	Reboot the handset. If the error repeats, contact Nortel Technical Support.
Select License	The correct protocol has not been selected from the license set.	Using the administrative menus, select one license from the license set to allow the wireless handset to download the appropriate software.
Server Busy	Wireless handset is attempting to download from a TFTP Server that is busy downloading other devices and refusing additional downloads.	None. The wireless handset will automatically retry the download every few seconds.
SKT Open Failed	Socket open fail. Occurs when the handset tries to connect to the call server, but there is not response. If resiliency is active, the handset will keep trying.	If the call server is inoperative and resiliency is not active, or the handset cannot locate a backup call server, turn off the handset and repair the primary call server. Note that it may be advisable to reconfigure the backup call server to be the primary call server if the repair is more time-consuming than the reconfiguration.
Storing Config	Handset is storing changes to handset configuration.	None. Informational message only. The handset may display this briefly following a configuration change or software download.

Table 22 Wireless handset status messages

Message	Description	Action
SVP Service Rej.	The WLAN IP Telephony Manager 2245 has rejected a request from the wireless handset.	The wireless handset restarts and attempts to re-register with the WLAN IP Telephony Manager 2245, which should fix the problem. Report this to the administrator if it keeps happening.
System Busy yyy.yyy.yyy.yyy (with busy tone)	y…y = SVP or GW IP Address Gateway or WLAN IP Telephony Manager has reached call capacity; displays the IP address of gateway/SVP Server.	All call paths are in use; try call again in a few minutes.
System Locked (with busy tone)	WLAN IP Telephony Manager 2245 is locked. Gateway is locked.	Try call again later. System has been locked for maintenance.
TFTP ERROR(x):yy	A failure has occurred during a TFTP software download. **(x)** = the file number that was being downloaded; **yy** = an error code describing the particular failure. Possible error codes are: 01 = TFTP Server did not find the requested file. 02 = Access violation (reported from TFTP Server). 07 = TFTP Server reported “No such user” error. 81 = File put into memory did not CRC. FF = Timeout error. TFTP Server did not respond within a specified period of time.	Error code 01, 02 or 07 – check the TFTP Server configuration. Error code 81 – the wireless handset will attempt to download the file again. For other messages, power off the wireless handset, then turn it on again to retry the download. If the error repeats, note it and contact Nortel Technical Support.
Too Many Errors	The handset continues to reset and cannot be recovered.	Fatal error. Return handset to Nortel.
Unknown xx:yy:zz	A phrase is missing from your phintl file.	Download new software from the Nortel site (see “Updating software” on page 113).

Table 22 Wireless handset status messages

Message	Description	Action
Updating Code…	Wireless handset is downloading new software into memory. The number icons at the bottom of the display indicate which file number is currently being downloaded. This message also displays a progress bar. When the progress bar fills the display line, the update operation is complete on that file.	None. When the progress bar fills the display line, the update operation is complete on that file. Do not turn off the handset during this operation.
VPN Error: xxxx	The VPN server returned an information message with a code of xxx.	
Waiting…	Wireless handset has attempted some operation several times and failed. It is now waiting for a period of time before attempting that operation again.	None. The wireless handset is waiting for a specified period of time before attempting that operation again.
Watchdog Timeout	The wireless handset failed to hear from the Call Server within the watchdog timeout interval.	Verify the Call Server is operational and connected to the network.
Wrong Code Type	The software loaded into the handset is incorrect for this model of handset.	Verify that the license type is set correctly. If the license type is correct, replace the software image on the TFTP server with the software that is correct for the handset model.

Using Call Server overlay commands

LD 32 IDU command

For the handsets, the IDU command outputs the following specific information:

- Release code: Rls: 6 (2210), Rls: 7 (2211) or Rls: 8 (2212)
- NT Code: NTTQ4010 (2210), NTTQ5010 (2211) or NTTQ69AA (2212)
- Software Version has different format: <Version>.<Issue>
  FW/SW:097.059 (or later)
- The IP address is the alias IP address of the wireless handset that is provided by the WLAN IP Telephony Manager 2245. The MAC address is the MAC address of the wireless handset. In other words, the MAC address and the IP address are not related.

In the following example, “61 0” is an IP Phone 2004 and “62 2” is a WLAN Handset 2211.

```
.idu 61 0
I2004 TN: 061 0 00 00 V
TN ID CODE: i2004
ISET MAC ADR: 00:60:38:76:41:C7
ISET IP ADR: 192 .168 .010 .100
LTPS IP ADR: 047 .011 .214 .165
MANUFACTURER CODE: [NAME]
MODEL:
NT CODE: NT2K00GI
COLOR CODE: 66
RLS CODE: 0
SER NUM: 7641C7
FW/SW VERSION: 0602B59
.idu 62 2
I2004 TN: 062 0 00 02 V
TN ID CODE: i2004
ISET MAC ADR: 00:90:7A:01:7E:47
ISET IP ADR: 192 .168 .010 .200
LTPS IP ADR: 047 .011 .214 .165
MANUFACTURER CODE: [NAME]
MODEL:
NT CODE: NTTQ5010
COLOR CODE: 66
RLS CODE: 7
SER NUM: 017E47
FW/SW VERSION: 097.021
```

LD 32 STAT command

The wireless handsets are shown REGISTERED in the standby and active modes. In the following example, “61 0” is an IP Phone 2004 and “62 2” is a WLAN Handset 2211 in the standby mode.

```
.stat 61 0
IDLE REGISTERED 00
.stat 62 2
IDLE REGISTERED 00
```

LD 117 Inventory command

In the inventory report, the wireless handsets have a specific release code and NT code, similar to the IDU command output. In the following example, “61 0” is an IP Phone 2004 and “62 2” is a WLAN Handset 2211.

```
=> inv prt sets
Set inventory:
17 10 2003 8 17 21, 17 10 2003 8 17 22, 6
i2004, 61 00, i2004 NT2K00GI 66 0 7641C7, I2004 , 6000
i2004, 62 02, i2004 NTTQ5010 66 7 017E47, I2211 , 6502
```

LD 117 STIP command

The STIP command can be used for wireless handsets; however, the wireless handset alias IP address is displayed as the TERMIP in the command output, instead of physical IP address. In the following example, the “192.168.10.200” is an alias IP address assigned by the WLAN IP Telephony Manager 2245.

```
TN          HWID                          STATUS HOSTIP       TERMIP         PORT
______ ________________________________ ______ _________ ____________ _______
0x600a 00000000000003000907a017e476607  REG  47.11.214.165 192.168.10.200 0x1450
CAPS

________
0x00000000
        --------------------------------
        codec bdwth(k) codecCaps desc
        --------------------------------
         4      190      0x00000000 1
         3      190      0x00000000 1
         17      47      0x00000001 1
value = 537232412 = 0x2005841C
```

Note: For information on more CLI commands, see to “Zones” on page 31.

TPS CLI commands

dsetShow command

In the dsetShow command output, the handsets have a specific Hardware ID. The alias IP address is output, not the physical wireless handset IP address.

In the following example, the IP Phone 2004 has an IP address of 192.168.10.100 and the WLAN Handset 2211 has an alias IP address of 192.168.10.200. The syntax of the Hardware ID is as follows:

- first two digits – Manufacturer Location. Manufacturer Location is 18 for the IP Phone 2004 and 30 for the WLAN Handset 2211.
- next six digits – Manufacturer Code. The Manufacturer Codes are defined as follows:
  - IP Phone 2004 Phase 1 – 006038
  - IP Phone 2004 Phase 2 – 000ae4
  - WLAN Handset 2210 – 00907a
  - WLAN Handset 2211 – 00907a
  - WLAN Handset 2212 – 00907a
- last two digits – Release Code. The Release Codes are defined as follows:
  - IP Phone 2004 Phase 1 – 0
  - IP Phone 2004 Phase 2 – 2
  - WLAN Handset 2210 – 0x06
  - WLAN Handset 2211 – 0x07
  - WLAN Handset 2212 – 0x08

```
-> dsetShow
TN    IP Address      Hardware ID       TermType
---- --------------- ------------------ ----------
6004 192.168.10.100 180060387641c76600  i2004
600A 192.168.10.200 3000907a017e476607  i2004
value = 0 = 0x0
```

e2dsetShow command

The e2dsetShow command is used for the handsets in the same manner as for the IP Phones.

isetCount / isetGet

Use the alias IP address of the handsets in the expression string of the isetCount and isetGet commands, not the physical IP address. The following is an example of the isetGet output for the WLAN Handset 2211.

```
->isetGet "IP == 192.168.10.200"
IP Address     Type  RegType  State Up Time   Set-TN  Regd-TN    HWID             FWVsn
----------     ----- -------   ----- ------- -------  -----    ------------       ---------
192.168.10.200 i2004 Regular online 0 00:12:00 062-02 062-02  3000907a017e476607   097.021


UNIStimVsn   SrcPort  DstPort
---------    ------   ------
  2.6         5100     5000
```

isetReset / isetResetAll

The isetReset command can be used to reset the wireless handsets by specifying the wireless handset alias IP, not the physical IP address:

```
-> isetReset "192.168.10.200"
value = 0 = 0x0
```

isetShow / isetShowByTN / isetShowByIP

Similar to the dsetShow command, the wireless handset outputs its specific hardware ID (see dsetShow) and alias IP, not the physical IP address. The
F/W version has a different format <Version>.<Issue> in this output.

In the following example, the telephone with TN "062-02" is the WLAN Handset 2211.

```
-> isetShow
Set Information
---------------
IP Address     Type  RegType State   Up Time     Set-TN  Regd-TN
----------     ----   -----   ----    -----       -----   -------
192.168.10.100 i2004 Regular online  4 22:59:22  061-00  061-00


   HWID              FWVsn   UNIStimVsn SrcPort DstPort
------------------    ----    --------   -----    -----
180060387641c76600   0602B59    2.8       5100    5000


IP Address     Type  RegType State   Up Time     Set-TN  Regd-TN
----------     ----   -----   ----    -----       -----   -------
192.168.10.200 i2004 Regular online 0 02:03:22 062-02 062-02


   HWID               FWVsn    UNIStimVsn SrcPort DstPort
-----------------     -----     -------    -----   ------
3000907a017e476607   097.021     2.6        5100    5000
```

umsKernalJobsShow / umsUpgradeAll

The umsKernalJobsShow and umsUpgradeAll commands cannot be used to monitor/originate software upgrades for wireless handsets since the wireless handsets are upgraded using a different mechanism without the help of the UMS subsystem. See the documentation for the TFTP server used by the wireless handsets to learn how to monitor/originate the software upgrade.

umsPolicyShow / umsUpdatePolicy

The IP Phone 2004 policy used in these commands is not applicable to handsets, even though they are configured as IP Phones 2004 in the IP Line software. The wireless handsets are upgraded using a different mechanism without the help of the UMS subsystem.

usiLibTrace

The usiLibTrace utility can be used to monitor UNIStim messages from the wireless handsets by entering the alias IP address, not the wireless handset physical IP address.

```
-> usiLibTraceOn "192.168.10.200", 255, 255
value = 0 = 0x0
```

Determining alias IP addresses

When diagnosing network problems, (for example, to "ping" the wireless handset), it is useful to know the mapping between the alias IP addresses as displayed by various Call Server commands and the physical IP address of the wireless handset. There is no single command that provides this information; however, the administrator can determine it in two ways:

1. If the wireless handset's IP address is statically configured, the administrator can look at the IP address of the wireless handset using the Admin menu, which is available when the wireless handset is powered on. See "Admin menu options" on page 65 for more information.
2. After the wireless handset is operating and in standby mode, the administrator can look at the User Preferences menu to find the alias IP address of the wireless handset. See "User-defined preferences" on page 107 for more information.

Troubleshooting coverage issues

Coverage issues are best resolved by adding and/or relocating APs. Overlap issues may be resolved by reassigning channels to the APs or by relocating the APs.

Before calling Nortel Technical Support

- To facilitate the handling of the call, obtain the following information and have it available when placing a call to Nortel Technical Support:
- software versions on the wireless infrastructure, such as the APs
- pre-installation site survey, including typical network information and the wireless site survey information from the site survey tool such as the Nortel Site Survey Tool
- paper-based layout of AP placement
- a more refined site survey of the area having issues using the wireless handset in Site Survey mode
- list of the PBX and LTPS software versions, including a list of patches
- WLAN IP Telephony Manager 2245 and handset firmware versions
- WLAN IP Telephony Manager 2245 configuration menu screen captures
- any error messages displayed in the Error Status screen of the System Status Menu of the WLAN IP Telephony Manager 2245

- any error messages displayed on the handset display screen
- content of the Syslog Server (if using)
- log of the DHCP Server (if available), if using DHCP

Appendix A
WLAN Application Gateway 2246

The WLAN Application Gateway 2246 is an optional device that enables third-party applications to communicate directly with a maximum of 10,000 handsets. The WLAN Application Gateway 2246 allows users to retrieve and respond to information using their wireless handsets.

The WLAN Application Gateway 2246 is available in several scaled capacity levels. The base unit NTTQ65AB enables 64 wireless handsets.

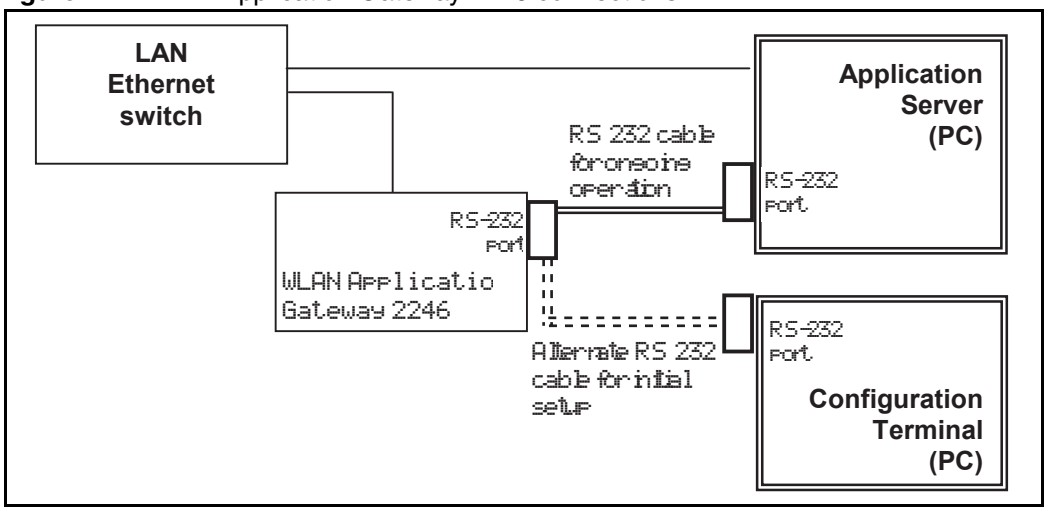
Table 23 Model numbers with maximum number of users

Model number	Maximum number of users
NTTQ65AB	64
NTTQ65BA	128
NTTQ65CA	256
NTTQ65DA	512
NTTQ65EA	1024
NTTQ65FA	10000

In Figure 22 on page 142, a WLAN Application Gateway 2246 is connected to the site's LAN through an Ethernet switch. The connection to the Application Server can be accomplished by a direct connection (RS-232) or through the Ethernet connection. Only one of these connections can be used at one time.

The IP address of the WLAN Application Gateway 2246 must be configured during initial configuration. After the IP address is established, the WLAN Application Gateway 2246 can be accessed by the Application Server through the RS-232 port or through the LAN using Telnet.

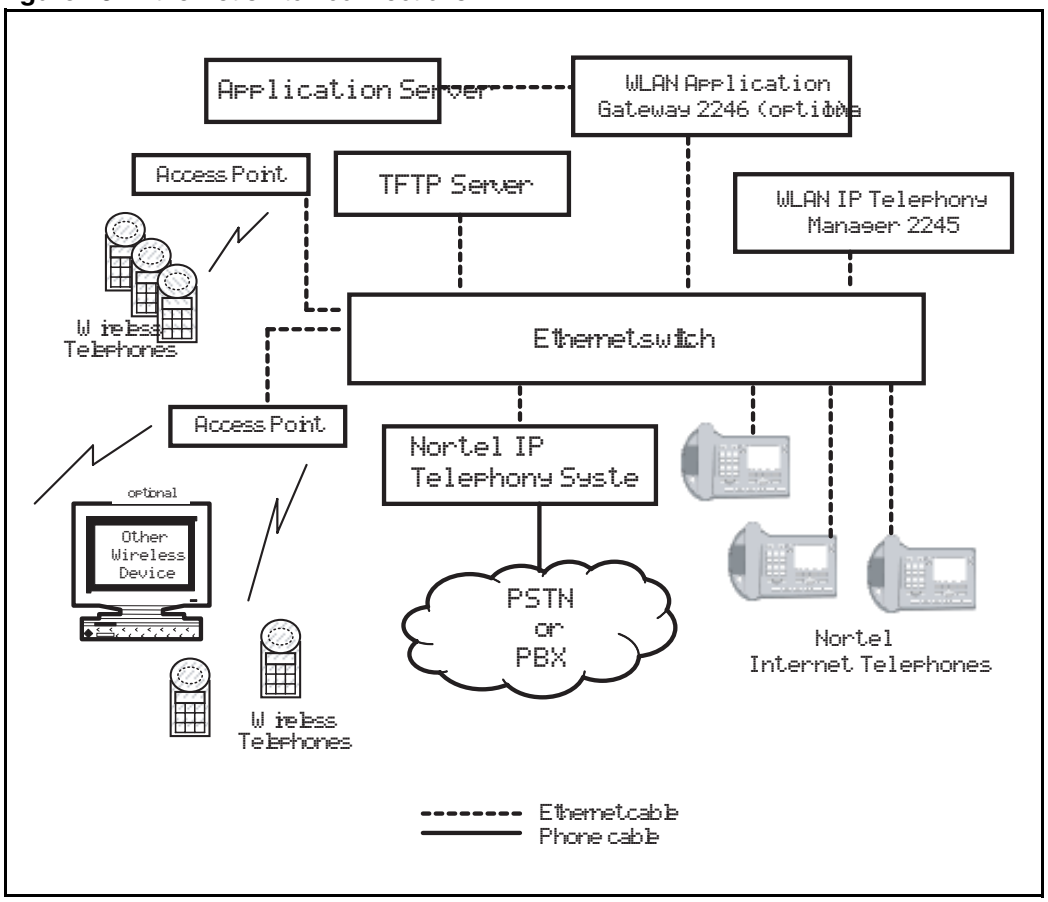
Figure 22 WLAN Application Gateway 2246 connections



System overview

At a typical site, the WLAN Application Gateway 2246 is connected to the Ethernet switch through an RJ-45/CAT 5 cable. The Application Server is connected through the RS-232 port. The client's system can include a LAN and its Application Server with a TAP connection to a communications device such as a paging controller.

Figure 23 Ethernet switch connections

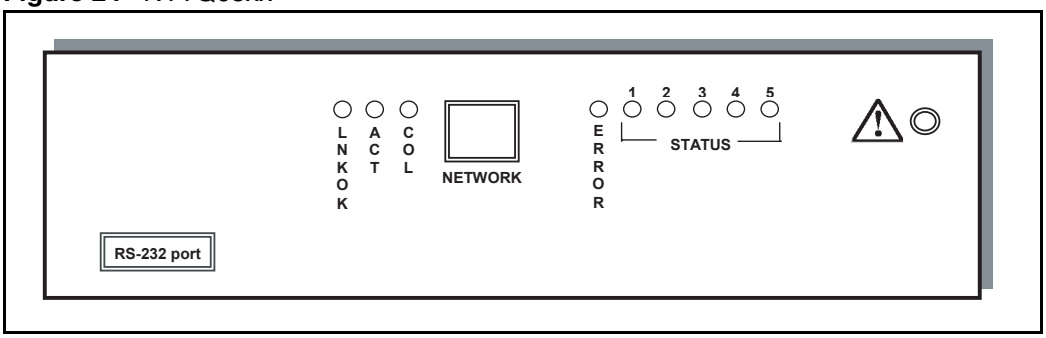


Front panel

The WLAN Application Gateway 2246 models have similar front panel indicators. See Figure 24.

The NTTQ65xx is available in scaled increments to support up to 10 000 users.

Figure 24 NTTQ65xx



- Network Link LEDs
  - **(L)NKOK** – lit when there is a network connection, (for example, LINK OK).
  - **(A)CT** – lit if there is system activity.
  - **(C)OL** – lit if there are network collisions.
  - **(E)RROR** – lit when the system has detected an error.
- Status LEDs – indicate system messages and status.
  - **1** – heartbeat, indicates the WLAN Application Gateway 2246 is running
  - **2, 3, and 4** – currently unused
  - **5** – System master

Third-party applications

The WLAN Application Gateway 2246 enables third-party software applications to communicate with the wireless telephones. Users can receive and retrieve important information from external systems. Some examples of applications in various markets are as follows:

Health care:

- access patient pharmaceutical records
- receive text messages from nurse call systems
- receive e-mail from remote test labs

Retail:

- look up merchandise prices
- access inventory

Manufacturing:

- relay alarms to handsets from malfunctioning equipment
- enable managers to monitor production output

Call Centers:

- review queue statistics
- receive alarms when metrics exceed thresholds

Nurse-call systems

In the health care market, the following nurse-call system manufacturers have applications known to be compatible with the WLAN Application Gateway 2246:

- Dukane Corporation
- Emergin Wireless Office
- Globestar
- Indyme Corporation
- Jeron Nurse Call
- OnSite Communications
- Rauland Nurse Call
- SoloTraxx
- Wescom Nurse Call

Installation

Installing with a new system

If this is a new system installation, complete "To install the WLAN Application Gateway 2246 when the rest of the system is tested.

Installing in an existing system

If the WLAN Application Gateway 2246 is being added to an existing system, the entire system must be reset before the WLAN Application Gateway 2246 can be used.

To install the WLAN Application Gateway 2246

1 Place the WLAN Application Gateway 2246 on a shelf or convenient location.

Note: The WLAN Application Gateway 2246 is physically connected to the Ethernet switch and can be placed in any convenient location within 325 ft (100 m) of the switch. It can also be rack-mounted.

2 Connect the power plug from the WLAN Application Gateway 2246 power adapter to the power jack on the front (or rear) of the box.

IMPORTANT!

Use only the power adapter provided by Nortel.

3 Plug the power adapter into an outlet or outlet strip.

4 Apply power to the WLAN Application Gateway 2246.

- Ensure that the ERROR LED is off.
- Ensure LED 1 is blinking.

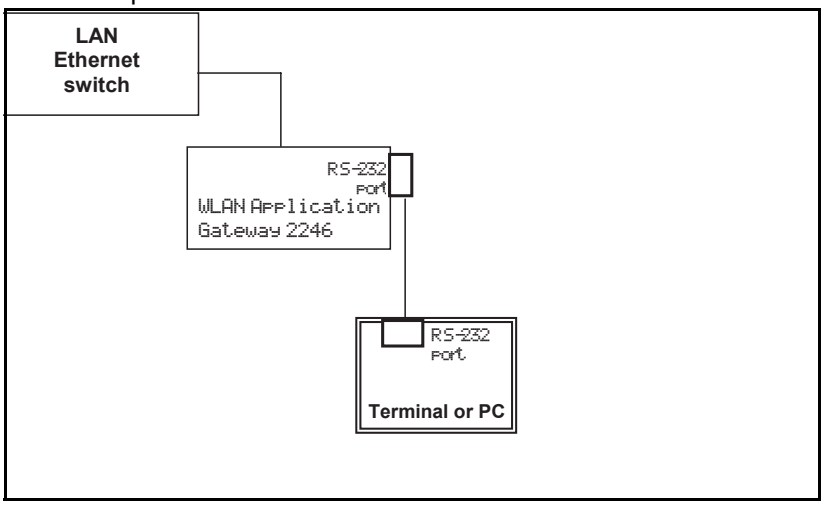
Configuring the WLAN Application Gateway 2246 IP address

It is necessary to connect to the WLAN Application Gateway 2246 through a serial connection to configure the IP address and the network parameters. Once this is done, administration and further configuration can be performed through a Telnet connection using the Administration Console.

To connect to the WLAN Application Gateway 2246 through a serial port

1 Using a DB-9 female, null-modem cable, connect the WLAN Application Gateway 2246 to the serial port of a terminal or PC. See Figure 25.

Figure 25 Cable to port connection



2 Run a terminal emulation program (such as HyperTerminal™) or use a VT-100 terminal with the following configuration:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Note: If using Windows 2000, Service Pack 2 must be installed to enable the use of HyperTerminal.

3 Reset the system.

The following displays on the terminal:

04830130

4 Type the following command using the terminal or PC keyboard:

0255CC [CTRL M] [CTRL J]

The command does not display on the screen as it is typed.

The Login prompt displays. If an error was made when entering the command string, the message “Ill Formed Packet” displays. It appears as a series of numbers followed by some form of the typed command. If this occurs, repeat Step 3 and Step 4.

5 Enter the default login **admin** and the default password **admin**.

Note: The login name and password are case-sensitive.

The **NetLink OAI System** screen appears. This screen, the main menu screen of the Administration Console, displays the factory-default name of the WLAN Application Gateway 2246 to which the serial port is connected. See Figure 26 on page 149.

Next, configure the WLAN Application Gateway (including IP address) by following the steps in the “Task summary list” on page 149.

Configuration

The NetLink OAI System screen is the main menu of the Administration Console. Use this screen to configure the WLAN Application Gateway 2246.

Navigating the Administration console

Use the keys described in Table 24 to move around the Administration console screens.

Table 24 Administration console navigation

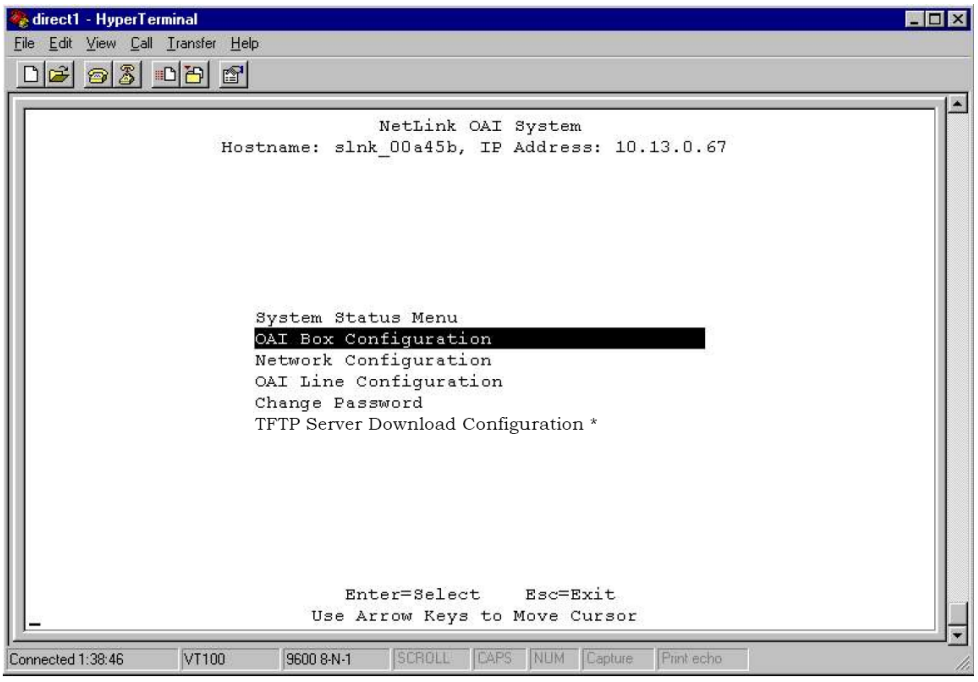
To perform this function.....	Press....
Select function from menu	Arrow keys to highlight the selection. Press **Enter.**
Display menu associated with highlighted field	**Enter**. The Enter key displays the options associated with an item or allows an entry to be typed into the field.
Exit screen	**Esc**. Press the Esc key to return to the previous screen.

Table 24 Administration console navigation

To perform this function.....	Press....
Move one line up	Corresponding arrow key.
Move one line down	
Move one field to the left	
Move one field to the right	
Scroll	If a screen has more lines of information than can be displayed at once, the text is wrapped. The scroll feature uses the arrow keys. Press the down arrow key at the last line to move the cursor to the top line. Press the up arrow key at the top line to move the cursor to the last line.

Note: The top line of each screen of the Administration Console displays the hostname and IP address of the WLAN Application Gateway 2246.

Figure 26 NetLink OAI System screen



Task summary list

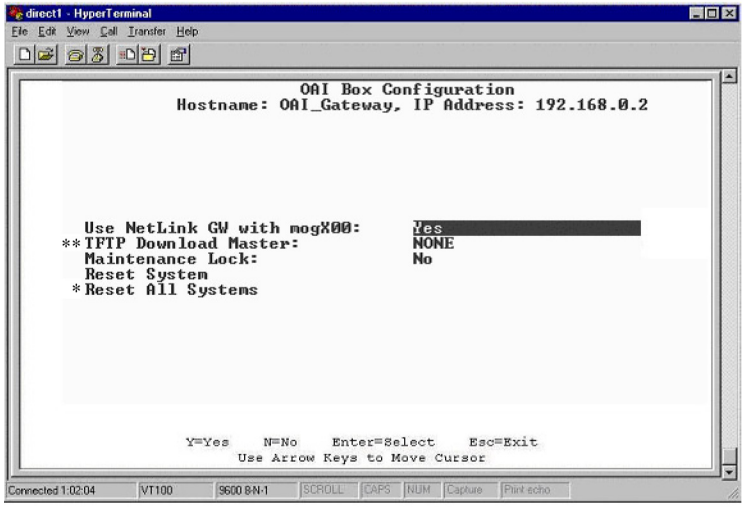
Complete the following tasks to configure the WLAN Application Gateway 2246:

1. Establish the system type from the OAI Box Configuration option. See "To configure the system type from the OAI Box Configuration option" on page 149.
2. Establish the Network settings from the **Network Configuration** option. See "Configuring the network" on page 55.
3. Configure the handsets from the Telephone Line Configuration option. See "Configuring the Telephone Line" on page 155.
4. Configure the function sequence that activates the application from the **Feature Programming** option. See "Programming a feature" on page 158.

To configure the system type from the OAI Box Configuration option

1. From the **NetLink OAI System** screen, select **OAI Box Configuration**.
2. The **OAI Box Configuration** screen displays. See Figure 27 on page 150.

Figure 27 OAI Box Configuration screen



Note: * – This option does not appear unless "Use NetLink GW with mogX00" is set to "Yes", as it is in this screen, which is the default.

3 Enter the configuration information for the WLAN Application Gateway 2246 (provided by the network administrator).

- **Use NetLink GW with mogX00** – change this option to No.
- **TFTP Download Master** – enter the IP address of the TFTP Server.
- **Maintenance Lock** – the system sets this option to Yes after maintenance activities have been performed that require a reset. This option cannot be changed. It is automatically set. Reset the system at exit to clear Maintenance Lock. Maintenance Lock prevents any new calls from starting.
- **Reset System** – if this option is set to Yes, the WLAN Application Gateway 2246 is reset after pressing ENTER.
- **Reset All Systems** – not applicable.

a Press **Esc** on the keyboard to return to the NetLink OAI System screen.

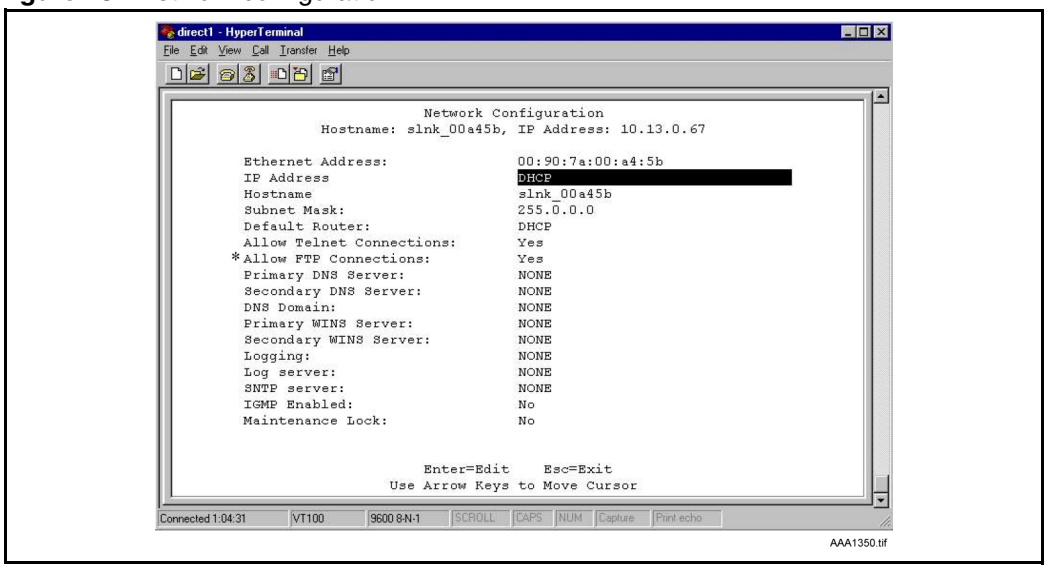
To configure the network

1 From the **NetLink OAI System** screen, select **Network Configuration**.

The Network Configuration screen appears. See Figure 28 on page 151.

Note: The **Allow FTP Connections** option appears only for NTTQ65xx models.

Figure 28 Network configuration



2 Enter the configuration information for the WLAN Application Gateway 2246, as provided by the network administrator.

- **Ethernet Address** – this is the MAC address of the WLAN Application Gateway 2246. This address is set at the factory.
- **IP Address** – enter the complete IP address for the WLAN Application Gateway 2246, including digits and periods. Do not use DHCP. The IP address can be changed after initial configuration.
- **Hostname** – the default host name can be changed. This is the name of the WLAN Application Gateway 2246 to which connection has been made. This name is for identification purposes only. Spaces cannot be entered in this field.
- **Subnet Mask** – Enter the subnet mask defined by the network administrator.
- **Default Router** – DHCP or static IP address.
- **Allow Telnet Connections** – Enter Y (Yes) to allow connection to the WLAN Application Gateway 2246 through Telnet. Enter N (No) if no Telnet connection is allowed.
- **Allow FTP Connections** – Yes/No (NTTQ65xx only).
- **DNS server and DNS domain** – these settings are used to configure Domain Name Services (DNS). (These settings can also be configured as DHCP. This causes the DHCP client in the WLAN Application Gateway 2246 to attempt to automatically obtain the correct configuration from the DHCP server. The DHCP setting is only valid when the IP address is also acquired using DHCP).
- **WINS servers** – these settings are used for Windows Internet Name Services (WINS). (These settings can also be configured as DHCP. This causes the DHCP client in the WLAN Application Gateway 2246 to attempt to automatically obtain the correct setting from the DHCP server. The DHCP setting is only valid when the IP address is also acquired using DHCP.) When WINS is configured properly, the WLAN Application Gateway 2246 can translate hostnames to IP addresses. When using Telnet, it is also possible to access the WLAN Application Gateway 2246 using its hostname instead of the IP address.

- **Logging** – can be configured to **Syslog** or **NONE**.
- **Log server** – enter the IP address or hostname of the Syslog server on the network if Syslog has been configured. The WLAN Application Gateway 2246 writes Syslog format diagnostic messages to the Syslog server.
- **SNTP server** – can be configured as a hostname, IP address, or NONE. The SNTP server is a Simple Network Time server. The WLAN Application Gateway 2246 obtains the current date and time from the SNTP server and tags syslog messages with the date.
- **IGMP Enabled** – configure as Yes or No. IGMP is Internet Group Routing Protocol. **IGMP Enabled** allows the WLAN Application Gateway 2246 to join multicast groups. Enable this option if the network switch connected to the WLAN Application Gateway 2246 requires IGMP for multicast traffic to be forwarded.
- **Maintenance Lock** – the system sets this option to Yes after maintenance activities have been performed that require a reset. This option cannot be changed. It is automatically set. Reset the system at exit to clear Maintenance Lock. Maintenance Lock prevents any new calls from starting.

3 Press **ESC** to return to the **NetLink OAI System** screen.

4 Reset the WLAN Application Gateway 2246.

To connect the WLAN Application Gateway 2246 to the LAN

1 Using an RJ-45 cable, connect the NETWORK port of the WLAN Application Gateway 2246 to the connecting port on the Ethernet switch.

2 Power up the entire system.

All components should cycle through their usual diagnostic routine.

Connecting to the Application Server

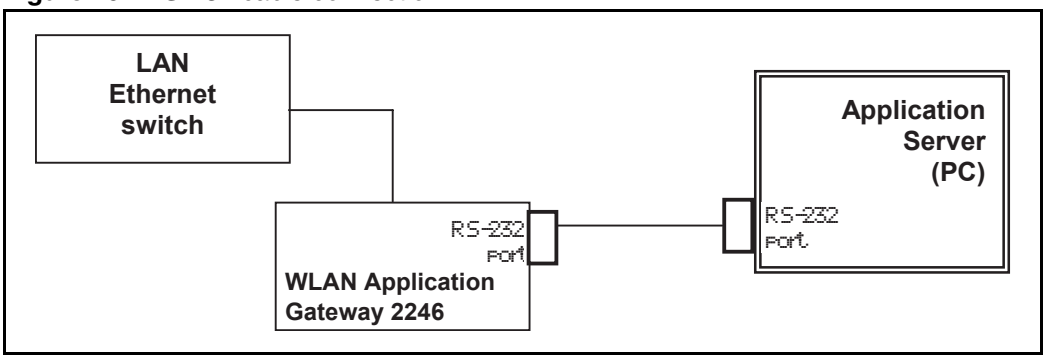
Some applications may require a LAN connection between the Application Server and the WLAN Application Gateway 2246. If the applications do not require a LAN connection, use the RS-232 port connection. In some situations, a modem is connected to be used for remote administration of the WLAN Application Gateway 2246.

Connect to the Application Server through an RS-232 port

Some applications or systems may require an RS-232 connection between the Application Server and the WLAN Application Gateway 2246. If the applications have the ability to communicate messages over TCP/IP, and do not require a serial connection, the RS-232 cabling is not required. In that case, the LAN connection (port 5456) through the Ethernet switch can be used for the applications.

Connect the Application Server to the WLAN Application Gateway 2246 serial port by using a cable that conforms to RS-232 standards for DTE-to-DTE connections (null modem cable).

Figure 29 RS-232 cable connection



The WLAN Application Gateway 2246 uses the following pins on the connector.

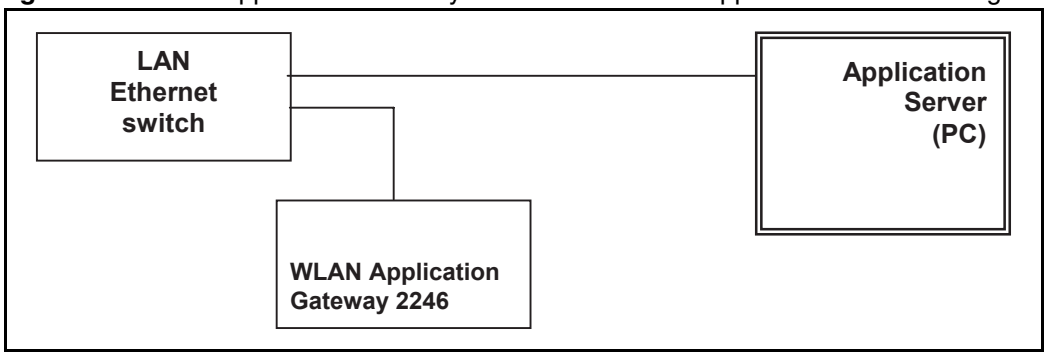
Table 25 Pins on the connector

Pin	Function
1	Carrier Detect
2	Data OAI Receives
3	Data OAI Transmits
5	Ground
7	Ready to Send
8	Clear to Send

Connect to the Application Server through the LAN

The IP address must be configured for the WLAN Application Gateway 2246 to function on the LAN. Follow the application's instructions to identify the WLAN Application Gateway 2246 to the application.

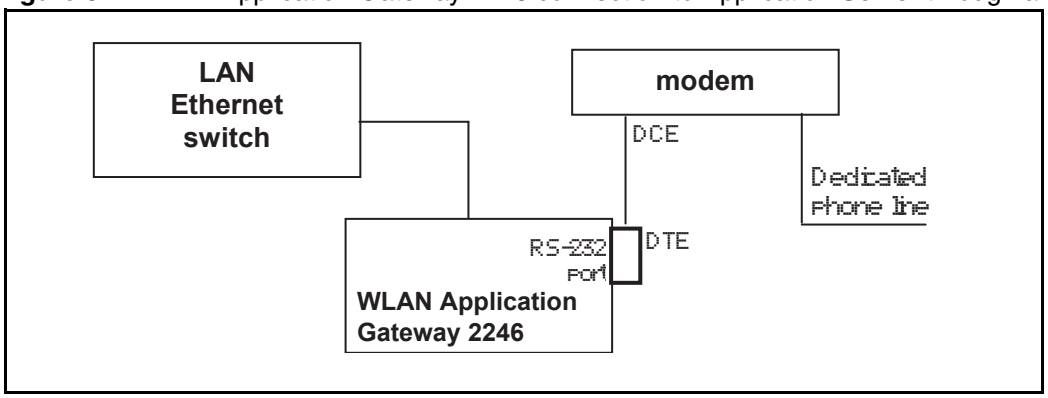
Figure 30 WLAN Application Gateway 2246 connection to Application Server through the LAN



Connect to Application Server through a modem

Connect the modem to the Gateway serial port using a cable that conforms to RS-232 standards for DTE-to-DCE connections. See Figure 31.

Figure 31 WLAN Application Gateway 2246 connection to Application Server through a modem



Continuing configuration through Telnet

After the IP address for the WLAN Application Gateway 2246 has been configured, the WLAN Application Gateway 2246 reset and connected to the LAN and the Application Server, Telnet can be used to continue the WLAN Application Gateway 2246 configuration.

Connecting through Telnet

Connection to the WLAN Application Gateway 2246 can be done through the network using Telnet. Telnet can only be used after the WLAN Application Gateway 2246 IP address has been configured.

The Telnet method of connection is used for routine maintenance of the system for both local and remote administration, depending on the network.

To connect to a WLAN Application Gateway 2246 through Telnet

1 Run a Telnet session to the IP address of the WLAN Application Gateway 2246.

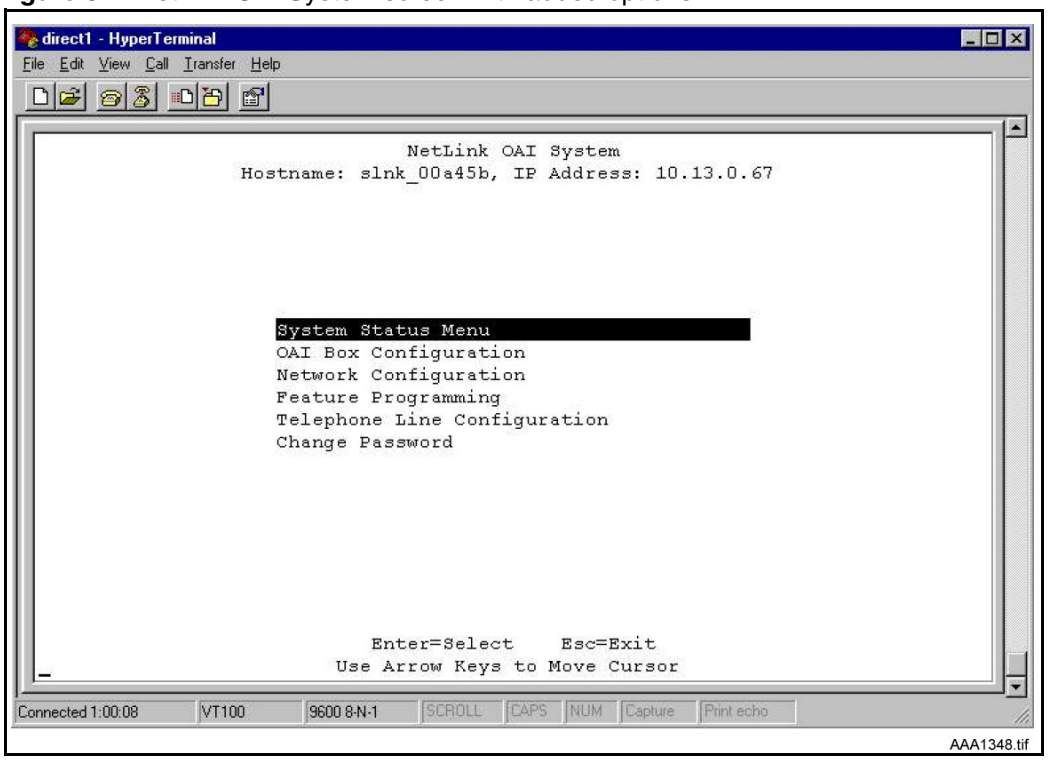
2 Log in to the WLAN Application Gateway 2246.

The **NetLink OAI System** screen appears.

Note: Since the WLAN Application Gateway 2246 has been initially configured, the NetLink OAI System screen now has some different options displayed.

When the configuration procedure is complete, the NetLink OAI System screen adds a Feature Programming option. Also, the OAI Line Configuration option is replaced by a Telephone Line Configuration option. See Figure 32 on page 155.

Figure 32 NetLink OAI System screen with added options



Configuring the Telephone Line

Each handset that uses the application features must be configured with its line number and MAC address. The name and extension number of the handset user can be entered. Obtain this information from the handset Planning Worksheet. See “Planning Worksheet for Handsets” on page 167.

The handsets require special configuration. This can include configuring options on the DHCP server or on the handset to allow it to communicate with the WLAN Application Gateway 2246. Be sure these setting are correct. See Chapter 7, “WLAN Handset configuration for more information.

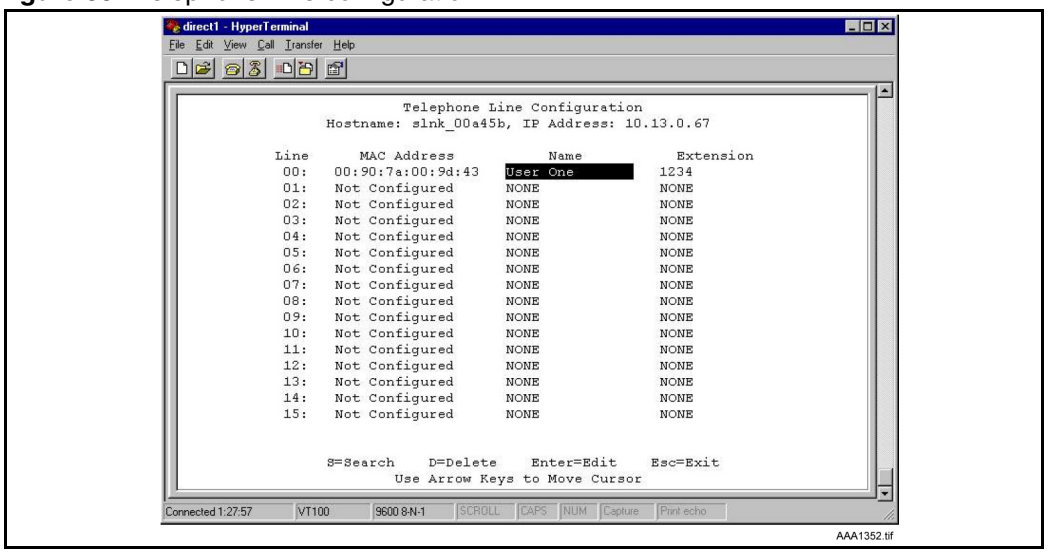
The system does not allow the same handset to register to two different lines. Use Esc to cancel any unwanted transaction.

To configure a telephone line

1 From the **NetLink OAI System** screen, select **Telephone Line Configuration** and press **Enter**.

The Telephone Line Configuration screen appears. See Figure 33 on page 156.

Figure 33 Telephone Line configuration


direct1 - HyperTerminal
File Edit View Call Transfer Help
Telephone Line Configuration
Hostname: slnk_00a45b, IP Address: 10.13.0.67
Line MAC Address Name Extension
00: 00:90:7a:00:9d:43 User One 1234
01: Not Configured NONE NONE
02: Not Configured NONE NONE
03: Not Configured NONE NONE
04: Not Configured NONE NONE
05: Not Configured NONE NONE
06: Not Configured NONE NONE
07: Not Configured NONE NONE
08: Not Configured NONE NONE
09: Not Configured NONE NONE
10: Not Configured NONE NONE
11: Not Configured NONE NONE
12: Not Configured NONE NONE
13: Not Configured NONE NONE
14: Not Configured NONE NONE
15: Not Configured NONE NONE
S=Search D=Delete Enter=Edit Esc=Exit
Use Arrow Keys to Move Cursor
Connected 1:27:57 VT100 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
AAA1352.tif

2 Use the arrow keys to navigate to the **Name** and **Extension** fields.

3 Enter the associated data for the wireless handsets.

- **MAC Address** – the MAC address is printed on the sticker underneath the battery on the handset. It can also be displayed on the handset by turning off the wireless handset, and then pressing and holding the Power On/Start Call button. The MAC address appears on the first line of the wireless handset display (12 characters). The MAC address must be manually entered by typing the entire address, including digits and colons.
- **Name** – enter the user name assigned to the wireless handset. This is for record keeping only; it does not communicate the name to the Call Server or the handset.
- **Extension** – enter the extension number assigned to the handset. This is for record keeping only; it does not communicate the extension number to the Call Server or the handset.

4 Write the MAC address on the Wireless Handset Planning Worksheet. See "Planning Worksheet for Handsets" on page 167.

5 Repeat step 4, step 5, and step 6 for each wireless handset to be added or changed.

6 Press **Esc** to return to the **NetLink OAI System** screen.

Deleting a handset

To delete a handset

1 From the **NetLink OAI System** screen, select **Telephone Line Configuration** and press **Enter**.

The Telephone Line Configuration screen appears.

2 Use the arrow keys to highlight the line to be deleted.

3 Press **D** to delete the handset information.

4 Press **Y** to accept changes.

5 Press **Esc** to return to the **NetLink OAI System** screen.

Searching for a handset

While in the Telephone Line Configuration or the Telephone Line Status screens, a search hotkey is available.

To search for a handset

1 From the **NetLink OAI System** screen, select **Telephone Line Configuration** and press **Enter**.

The Telephone Line Configuration screen appears.

2 Select the field to use as the search key (**MAC Address**, **Name**, or **Extension**),

3 Press **S** to display a search screen dialog box.

4 Type an appropriate search string.

5 Press **Enter**.

The success or failure of the search is displayed at the bottom of the screen.

6 Continue to change the search string for different search criteria or exit by pressing the Esc key.

The first line of the Telephone Line Configuration or Telephone Line Status screen displays the line in which the search match is found.

Successful searches always have the first found match at the top of the list.

Note: Partial strings match the beginning of strings. For example, a search for extension 10 matches extensions 10, 100, 1000, and so on, but will not match 010.

Programming a feature

The application function is accessed in the handset by pressing the FCN button plus a second button. The button used to access the application feature from the wireless handset is configured through the Feature Programming option.

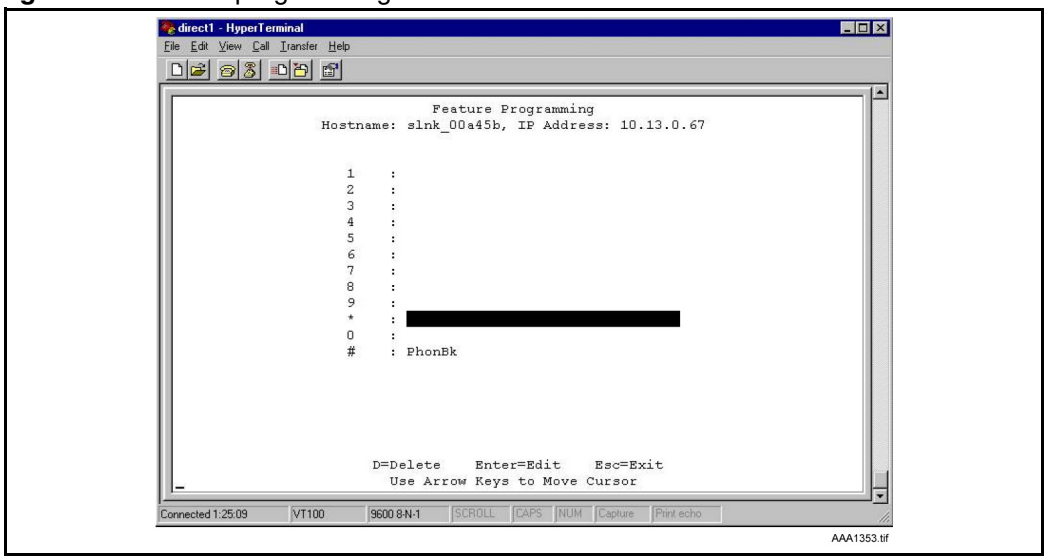
Note: FCN 1-6 are hard-coded. If the application function is programmed to use FCN 1-6, the hard-coded function is overridden. Nortel recommends using 7, 8, or 9 for the application function.

To program a feature

1 From the **NetLink OAI System** screen, select **Feature Programming** and press **Enter**.

The Feature Programming screen appears. See Figure 34.

Figure 34 Feature programming screen



2 Use the arrow keys to select the function number 7, 8, or 9 to associate with the application.

3 Type any label up to six characters.

The label typed here is displayed on the handset telephone display screen next to the assigned number on the FCN menu.

In Figure 34, the FCN + # key sequence displays PhonBk on the handset function menu. Figure 34 displays an application; in this case, a phone book enabling speed dialing to those listed.

Setting or changing a password

A unique password can be configured for the WLAN Application Gateway 2246. The password restricts access to the device's administrative functions.

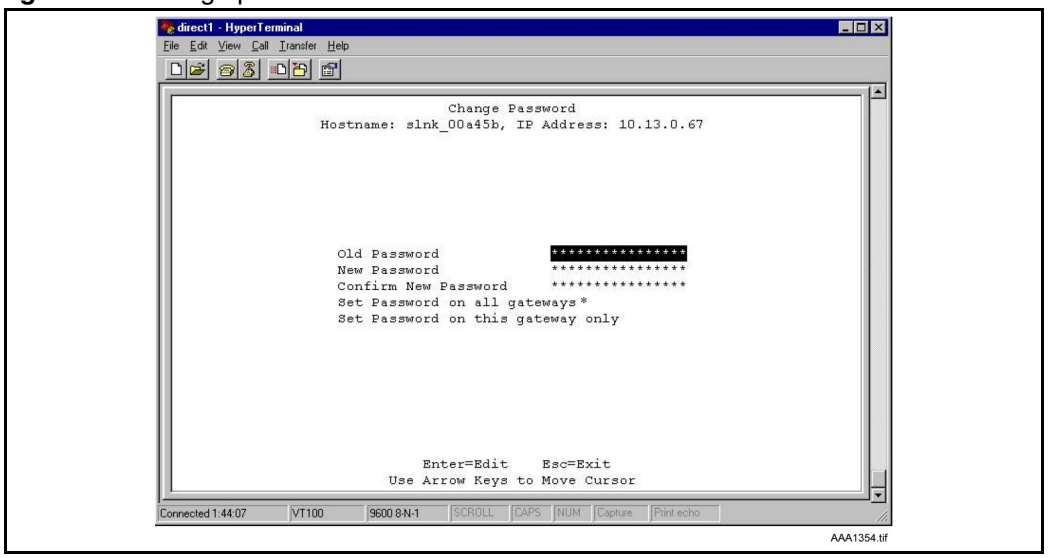
Warning: Record the password and store it in a safe place. If the password is lost or forgotten, contact Nortel Technical Support.

To set or change a password

1 From the **NetLink OAI System** screen, select **Change Password** and press **Enter**.

The Change Password screen appears. See Figure 35.

Figure 35 Change password



Note: * - not applicable.

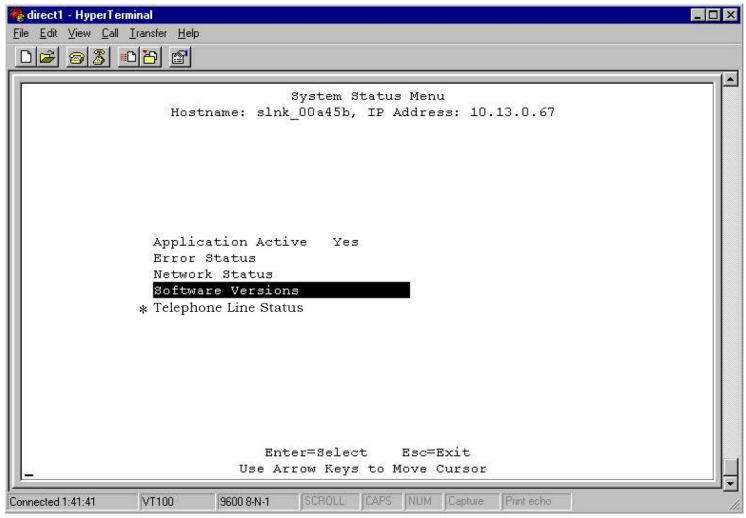
2 Use the default password **admin**.

3 Follow the prompts to configure a new password.

Viewing system status

To view the status of the system, select the System Status Menu option from the NetLink OAI System screen. The Systems Status Menu screen displays. See Figure 36 on page 160.

Figure 36 System Status Menu screen



The following options can be selected:

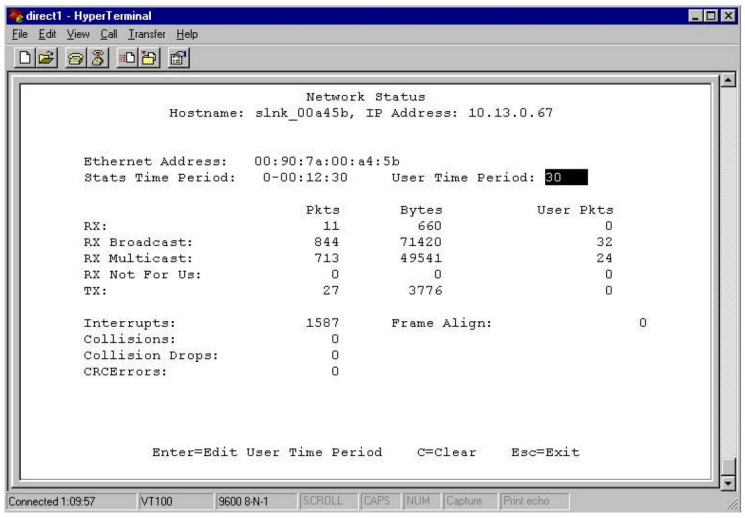
- **Application Active** – displays **Yes** when the application is communicating correctly with the WLAN Application Gateway 2246. Displays **No** when the application is not connected. This field is read-only and changes dynamically.
- **Error Status** –The only application-specific error is **No ECP heartbeat**, which means the application failed to send a heartbeat to the WLAN Application Gateway 2246.
- **Network Status** – information about the connection to the LAN. See "Viewing network status" on page 160.
- **Software Versions** – lists the software versions currently running on the WLAN Application Gateway 2246. See "Viewing software versions" on page 163.
- *** Telephone Line Status** – information about the functioning of each wireless handset registered to the WLAN Application Gateway 2246. See "Viewing Telephone Line Status" on page 162.

Viewing network status

The WLAN Application Gateway 2246 is connected to the Ethernet network, referred to as the LAN. The information about this connection displayed on the Network Status screen.

From the System Status Menu screen, select Network Status. The Network Status screen displays information about the Ethernet network. This information can help troubleshoot network problems. See Figure 37 on page 161.

Figure 37 Network Status


direct1 - HyperTerminal
File Edit View Call Transfer Help
Network Status
Hostname: slnk_00a45b, IP Address: 10.13.0.67
Ethernet Address: 00:90:7a:00:a4:5b
Stats Time Period: 0-00:12:30 User Time Period: 30
Pkts Bytes User Pkts
RX: 11 660 0
RX Broadcast: 844 71420 32
RX Multicast: 713 49541 24
RX Not For Us: 0 0 0
TX: 27 3776 0
Interrupts: 1587 Frame Align: 0
Collisions: 0
Collision Drops: 0
CRCErrors: 0
Enter=Edit User Time Period C=Clear Esc=Exit
Connected 1:09:57 VT100 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
AAA1356.tif

The following information is displayed at the top of the screen:

- **Ethernet Address** – MAC address of the WLAN Application Gateway 2246 (hexadecimal).
- **Stats Time Period** – the length of time the statistics have been accumulating in the **Pkts** and **Bytes** columns. This is either the system uptime, or the time that has elapsed since a user pressed **C=Clear** while viewing this display.
- **User Time Period** – the length of time (in seconds) that statistics accumulate in the Userpkts column before resetting to zero. When troubleshooting a problem, use this setting to isolate statistics for a given time period (for example, one hour). This is the only field in this screen that can be changed by the user.

The rest of the display is a table of Ethernet statistics. The Pkts and User Pkts columns list the count of Ethernet packets received or transmitted. The Bytes column is the count of bytes received or transmitted during the amount of time indicated by the Stats Time Period.

- **RX** – number of packets and bytes received addressed to the WLAN Application Gateway 2246.
- **RX Broadcast** – the number of broadcast packets and bytes received.
- **RX Multicast** – the number of packets and bytes received with the multicast address. (A “multicast” message is sent to more than one destination on the network.)
- **RX Not For Us** – the number of multicast packets and bytes received that were not for the WLAN Application Gateway 2246.
- **TX** – the total number of packets and bytes transmitted.
- **Interrupts** – the number of times the Ethernet controller signals the microprocessor that it has received or sent a packet.
- **Collisions** – the number of times the Ethernet controller attempts to send a packet, but another device on the network transmitted at the same time, corrupting the transmission.

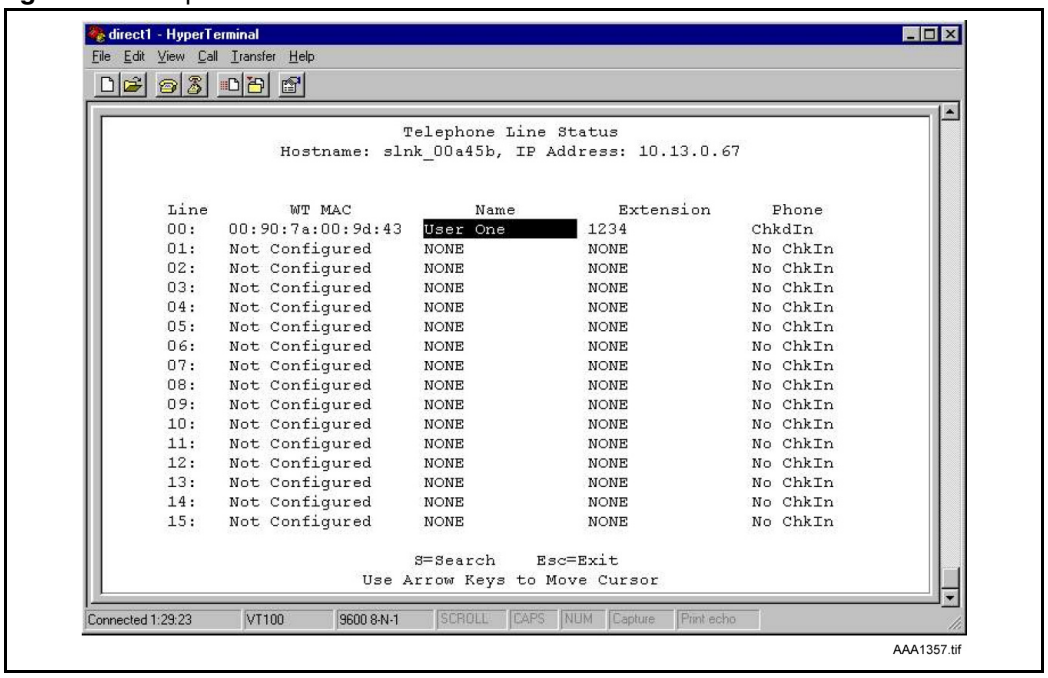
- **Collision Drops** – the number of packets the Ethernet controller discards, because there were over sixteen collisions. After sixteen collisions, the Ethernet controller hardware discards the current packet and attempts to send the next packet in its buffer.
- **CRC Errors** – the number of packets discarded by the Ethernet controller, because of a cyclic redundancy check (CRC) error.

Viewing Telephone Line Status

The Telephone Line Status screen displays which wireless handsets are communicating with the WLAN Application Gateway 2246.

From the System Status Menu screen, select Telephone Line Status. The WLAN Application Gateway 2246 displays up to 16 telephone lines at one time. See Figure 38. Move to the next group of 16 lines by using the arrow keys.

Figure 38 Telephone Line Status screen


direct1 - HyperTerminal
File Edit View Call Transfer Help
Telephone Line Status
Hostname: slnk_00a45b, IP Address: 10.13.0.67
Line WT MAC Name Extension Phone
00: 00:90:7a:00:9d:43 User One 1234 ChkdIn
01: Not Configured NONE NONE No ChkIn
02: Not Configured NONE NONE No ChkIn
03: Not Configured NONE NONE No ChkIn
04: Not Configured NONE NONE No ChkIn
05: Not Configured NONE NONE No ChkIn
06: Not Configured NONE NONE No ChkIn
07: Not Configured NONE NONE No ChkIn
08: Not Configured NONE NONE No ChkIn
09: Not Configured NONE NONE No ChkIn
10: Not Configured NONE NONE No ChkIn
11: Not Configured NONE NONE No ChkIn
12: Not Configured NONE NONE No ChkIn
13: Not Configured NONE NONE No ChkIn
14: Not Configured NONE NONE No ChkIn
15: Not Configured NONE NONE No ChkIn
S=Search Esc=Exit
Use Arrow Keys to Move Cursor
Connected 1:29:23 VT100 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
AAA1357.tif

The following information is displayed on the Telephone Line Status screen:

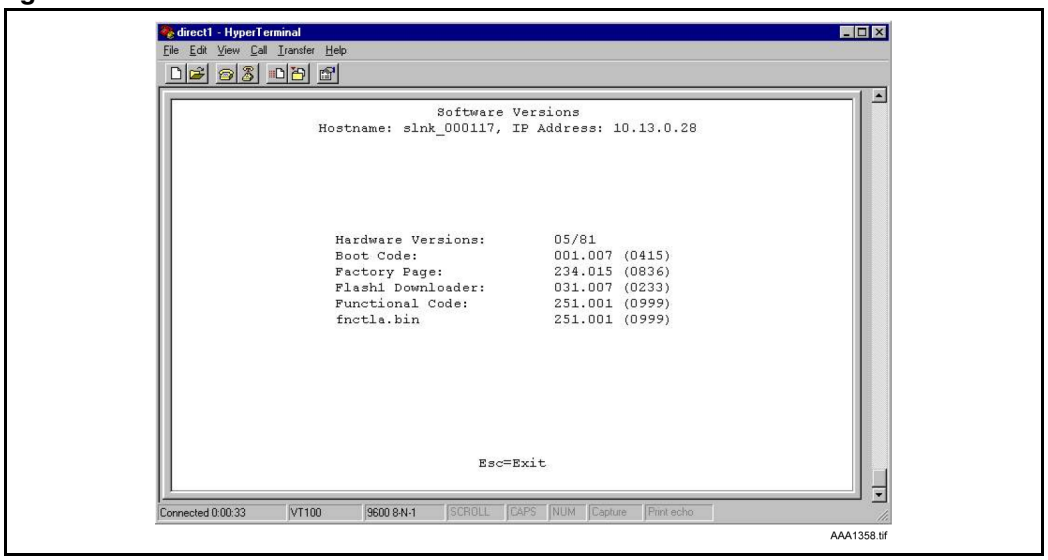
- **WT MAC** – the MAC address of the handset that was entered when the wireless handset was configured.
- **Name/Extension** – these fields contain the data entered at configuration.
- **Phone** – No ChkIn indicates the handset is not using the application function. ChkIn indicates the handset is communicating with the WLAN Application Gateway 2246.

Viewing software versions

Each WLAN Application Gateway 2246 and handset runs software that is controlled and maintained through versioning. The **S**oftware Versions screen provides information about the version currently running on the components. This information helps determine if the most recent version of software is running, and assists Nortel Technical Support in troubleshooting software problems.

From the System Status Menu screen, select Software Versions. The Software Versions screen displays. See Figure 39.

Figure 39 Software Versions screen



Certification testing

WLAN Application Gateway 2246 certification

When the WLAN Application Gateway 2246 is properly connected to the Application Server, LED 1 blinks.

Wireless handset certification

WLAN Application Gateway 2246 installation on new system

If this is a new system installation, continue with handset registration and Call Server programming. When the wireless handset installation is complete, perform the usual voice and coverage tests.

WLAN Application Gateway 2246 installation on existing system

To certify wireless handsets on an existing system

1. Place a test call.
2. Test the features on each handset to ensure the system is working properly.
3. Test the application on each handset.
4. Consult the application provider for specific test procedures.

Updating software

The WLAN Application Gateway 2246 and the handset use proprietary software programs. The software versions that are running on the system components can be displayed through the System Status screen.

Nortel provides information about software updates, and how to obtain the software (for example, downloading from the Nortel web site).

Software updates

After obtaining the software updates from Nortel, they must be transferred to the appropriate location in the LAN. This enables the corresponding system components to access and update their software. The FTP (File Transfer Protocol) method of transfer is used.

In the WLAN Application Gateway 2246, the flash file system has the following files:

Table 26 Software files

File name	Description
config.bin	OAI box configuration
fnctla.bin	functional code
oaiptlst.bin	phone list configuration
oaipttlsb.bin	redundant phone list configuration

Nortel periodically upgrades the fnctla.bin file, which is the only file downloaded. The other files are configuration files and their names are provided for information and backup purposes.

Obtain software using FTP

When using FTP, a host system is used to connect to a remote system. In this example, the host is the client and the server is the WLAN Application Gateway 2246. The “put” command means to copy the files from the host to the remote system.

Note: FTP commands vary with the particular FTP program used. Use the following steps as a general guide but be aware that an FTP program may use different terms to describe the procedure.

Transferring the software using FTP

1 Navigate to the OAI Box Configuration screen and place the system in Maintenance Lock before proceeding with the FTP procedure.

Note: This prevents new calls from starting. No calls may be in progress during the FTP procedure.

2 Connect to the WLAN Application Gateway 2246 using the command: **FTP <hostname>** or **FTP <IP address>**.

3 Log in using the administrator login **admin** and password (default is **admin**).

Result: A login confirmation message displays, followed by the FTP> prompt.

4 At the FTP prompt, type **binary**.

Result: A confirmation message displays.

5 At the FTP prompt, use the **put** command to transfer the functional code file to the client server or WLAN Application Gateway 2246.

Rename the file before loading it into the WLAN Application Gateway 2246. The download file is named **MOG700.bin**. Rename the file **fnctla.bin**.
Example: put mog700.bin fnctla.bin

6 After files are transferred, use the **Quit** command to quit FTP.

7 Navigate to the **NetLink OAI System** screen for the WLAN Application Gateway 2246

8 Select **System Status**.

9 Select **Software Versions** to verify that software versions for the WLAN Application Gateway 2246 are correct.

10 Reset the system through the **OAI Box Configuration** screen in order to restore Maintenance Lock to “N”.

Note: A GUI FTP client can be utilized instead of the described command line FTP procedure.

TFTP software updates Systems

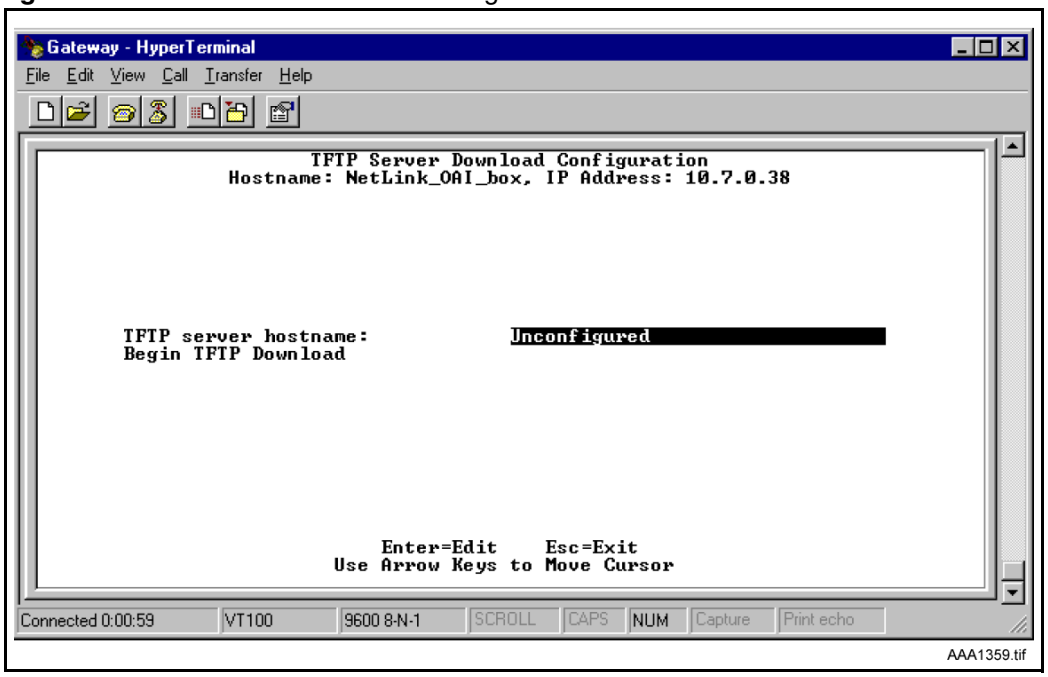
The WLAN Application Gateway 2246 uses proprietary software programs. The software versions running on the system components can be displayed through the WLAN Application Gateway 2246's **System Status** screen.

Nortel provides information about software updates and how to obtain the software (for example, downloading from the Nortel web site).

To load software updates

1. Install a TFTP Server on a LAN-connected system.
2. Consult the server vendor's documentation for information about TFTP.
3. After obtaining the software update from Nortel, load the software in a location that is accessible by the TFTP program.
4. To configure the host and start the download, select the **TFTP Server Download Configuration** option from the **NetLink OAI System** screen. See Figure 40.

Figure 40 TFTP Server Download Configuration screen



5. Enter the TFTP Server hostname.
6. Use the arrow keys to move the cursor to the **Begin TFTP Download** option.
7. Press **Enter** to begin the download.

   The code downloads into the WLAN Application Gateway 2246.

Planning Worksheet for Handsets

Copy and complete the worksheet in Table 27 to track parameters for each handset.

Table 27 Handset Planning Worksheet

OAI Port	MAC Address	User Name	Dialing Ext.	IP Address (if static)
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				

Table 27 Handset Planning Worksheet

OAI Port	MAC Address	User Name	Dialing Ext.	IP Address (if static)
29				
30				

Freeing the serial port for administrative purposes

If the serial port is being used as the primary communication link with the Application Server, it is necessary to enter the OAI command to free the serial port to allow it to be used for administrative purposes, such as changing the IP address of the WLAN Application Gateway 2246.

To free the serial port to allow it to be used for administrative purposes, follow the steps in "To use the serial port as the Application Server communication link.

After configuring the WLAN Application Gateway 2246, perform the following steps to again use the serial port as the communication link with the Application Server.

To use the serial port as the Application Server communication link

1. Disconnect the terminal or PC from the serial port on the WLAN Application Gateway 2246.
2. Reconnect the communication cable between the WLAN Application Gateway 2246 and the Application Server.
3. Reset the system.

   Normal communication between the Application Server and WLAN Application Gateway 2246 commences.

Appendix B
Compatible Access Points

All SpectraLink SVP- or VIEW-compatible Access Points (AP) are supported. Refer to the SpectraLink web site for details on the supported APs. The SpectraLink web site also contains configuration notes for the compatible APs.

Index

Numerics

10 dBm 104
10 Mb/s 36
50 msec 43
70 msec 43
802.1 p/q 45
802.1p tagging 45

A

Access Points (APs)
Configuration notes 74, 75
Admin menu 64
Admin Password 64
Administration Console navigation 147
alarms 118
alarms on the WLAN IP Telephony Manager 2245 118
alarms, active 118

C

Call Server 109
change subnets 72
channel conflicts 104
channel overlaps 104
checking in 109
Codecs 43, 80
Configuration notes 74, 75
copyright 2

D

DHCP 36
DiffServ 45
duplex mismatch 31, 121, 122

E

Error Status screen 118
European Regulatory rules 77
External Applications Server 45

F

filters 35
France 77
Full-duplex 31

G

G.711 43
G.723.1 43
G.729A 43
G.729B 43
Gain adjustment 44
gateway 34, 45, 51, 109, 110

H

half-duplex 36

I

IP Phone 2004 80, 83, 84, 85
ISM parameters 18

J

jitter 43
jitter buffer 43

L

Language 18
latency 43
Layer 2 port 45
Layer 2 QoS 45
Layer 2 switch port 45
Layer 3 port 45
License Option 69
locking the WLAN IP Telephony Manager 2245 113
loss plan 44
LTPS 109

M

mapping 80
master WLAN IP Telephony Manager 2245 33, 111
multicast addresses 35
Multicasting 35

N

network segments 35
No ring 122

node 43
non-master WLAN IP Telephony Server 2245 33

O

OAI 69
OAI On/Off 69
overlaps 104

P

packet loss 43
Planning worksheets 37
prevent new calls from starting 113
priority 45
Programmable rings and tones 44
Push-to-talk (PTT) 19, 35, 70, 105

R

rack-mount unit 36
Receive Loudness Rating (RLR) 43
refresh 24
Regulatory Domain 77
regulatory information 2
related publications 14
remote endpoint 43
reset the WLAN IP Telephony Manager 2245 113
Restore Defaults 78
RLR 43
Roaming 34
roaming 72
Routers 35
RTCP 43
RTP 43
Run Site Survey 77

S

Security 73
  Virtual Private Network (VPN) 19, 75
  Wi-Fi Protected Access (WPA) 19, 74
  Wi-Fi Protected Access2 (WPA2) 19, 75
  Wired Equivalent Privacy (WEP) 19, 73
Send Loudness Rating (SLR) 43
Site Survey mode 104
SLR 43
software updates 113
software versions 113
Spain 77
subnet 35
SVPServer
  Mounting 49

T

TFTP 113
Timing function 34
tone capability 44
trademarks 2
troubleshooting 31, 109

U

UNIStim 43, 45
unzipped 24
Update software 113

V

Virtual Private Network (VPN) 19, 75
VLAN 35
voice mail 122

W

Wi-Fi Protected Access (WPA) 19, 74
Wi-Fi Protected Access2 (WPA2) 19, 75
Wired Equivalent Privacy (WEP) 19, 73